MARK J. BOURASSA, ESQ. (NBN 7999)
JENNIFER A. FORNETTI, ESQ. (NBN 7644)
VALERIE S. CHRISTIAN, ESQ. (NBN 14716)
THE BOURASSA LAW GROUP
2350 W. Charleston Blvd., Suite 100
Las Vegas, Nevada 89102
Telephone: (702) 851-2180
Facsimile: (702) 851-2189
Email: *mbourassa@blgwins.com*
jfornetti@blgwins.com
vchristian@blgwins.com

NICHOLAS A. COLELLA (*pro hac vice*)
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, Pennsylvania 15222
Telephone: (412) 322-9243
Email: *nickc@lcllp.com*

Co-Interim Counsel for Plaintiffs and the Class

[additional counsel in signature block]

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA
***

IN RE HANKINS PLASTIC SURGERY ASSOCIATES, P.C. dba HANKINS & SOHN PLASTIC SURGERY ASSOCIATES This Document Relates to: All Actions	Master file No. 2:23-cv-00824-RFB-DJA **SECOND AMENDED CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs JENNIFER TAUSINGA, ALYSIA WRENN, OLGA ROMASHOVA, CAROLINE AURORA, SARAH JEFFERSON (collectively, "Plaintiffs"), bring this Second Amended Consolidated Class Action Complaint on behalf of themselves, and all others similarly situated, against Defendant Hankins Plastic Surgery Associates P.C. dba Hankins & Sohn Plastic Surgery Associates ("Hankins" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to themselves, which are based on personal knowledge:

NATURE OF THE ACTION

1. Healthcare providers that handle sensitive, personally identifying information ("PII") or protected health information ("PHI") owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII or PHI to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private health matters.

2. The harm resulting from a data and privacy breach manifests in a number of ways, including identity theft and financial fraud, and the exposure of a person's PII or PHI through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional prophylactic measures.

3. Hankins is a healthcare provider with locations in Henderson and Las Vegas, Nevada. Hankins provides plastic surgery care to patients across the greater Las Vegas Valley.[1]

4. As a healthcare provider, Hankins knowingly obtains, collects, and stores patient PII and PHI. In turn, Hankins has a resulting duty to secure, maintain, protect, and safeguard the PII and PHI that it collects and stores against unauthorized access and disclosure through reasonable and adequate data security measures.

5. Despite Hankins' duty to safeguard its patients' PII and PHI, Plaintiffs' and other patients' PII and/or PHI was exfiltrated by a threat actor during a data breach of Defendant's computer network which occurred on or around February 23, 2023 (the "Data Breach").[2]

6. On or about March 14, 2023, Hankins began notifying affected patients and/or prospective patients, including Plaintiffs of "a recent data security event that may impact some of your information.

---

[1] *Hankins Plastic Surgery Center*, https://www.hankinsplasticsurgery.com/ (last visited Sept. 15, 2023).

[2] *Notice of Security Incident/Data Breach*, Hankins & Sohn Plastic Surgery Associates (Apr. 3, 2023), https://ago.vermont.gov/sites/ago/files/2023-04/2023-04-03%20Hankins%20%26%20Sohn%20Plastic%20Surgery%20Associates%20Data%20Breach%20Notice%20to%20Consumers.pdf ("Notice of Data Breach").

We are providing you with information about the event, our response, and steps you can take to better protect your information against the possibility of misuse of your information, should you feel it appropriate to do so. We recently became aware of allegations by an unknown actor that data was stolen from our network. We are working diligently to assess these allegations and to confirm the nature and scope of the activity. We are also actively working with law enforcement to investigate the activity. We are reviewing the information that we store on our systems to identify current and former patients whose information may have been impacted by this event. …" A copy of one of these emails is attached as **Exhibit "1."**

7. When notifying its patients of the Data Breach, Hankins further warned that the threat actor intended to misuse the exfiltrated patient PII and PHI to commit extortion, informing patients that the threat actor "threatened to reach out to our patients individually." *See* **Exhibit "1."**

8. Based on the public statements of Hankins to date, a wide variety of patient PII and PHI was implicated in the Data Breach, including but not limited to patient names, contact information, dates of birth, Social Security Numbers, driver's license information, medical history, consultation notes, and photos.

9. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect patient PII and/or PHI. Defendant disregarded the rights of Plaintiffs and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard patient PII and/or PHI; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to monitor and timely detect the Data Breach.

10. As a result of Defendant's failure to implement and follow basic data security procedures, Plaintiffs' and Class Members' PII and PHI is now in the hands of cybercriminals who wish to use it for nefarious purposes.

11. Plaintiffs and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, and similar forms of criminal mischief, risks which may last for the rest of

their lives. Consequently, Plaintiffs and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

12. Plaintiffs, on behalf of themselves and all others similarly situated, allege claims for negligence, breach of implied contract, unjust enrichment, breach of confidence, violations of the Nevada Consumer Fraud Act, negligent misrepresentation, and seek to compel Defendant to adopt reasonably sufficient security practices to safeguard patient PII and PHI that remains in its custody in order to prevent incidents like the Data Breach from reoccurring in the future and to further provide Plaintiffs and Class Members with credit monitoring services for the rest of their lives.

PARTIES

13. Plaintiff Jennifer Tausinga is and, at all relevant times hereto, an adult who is a citizen and resident of the State of Nevada.

14. Plaintiff Tausinga is a patient of Hankins. On or about March 14, 2023, Plaintiff Tausinga received a notification from Defendant indicating that her PII and/or PHI may have been affected by the Data Breach.

15. Plaintiff Alysia Wren is and, at all relevant times hereto, an adult who is a citizen and resident of the State of Nevada.

16. Plaintiff Wrenn is a patient of Hankins. On or about March 14, 2023, Plaintiff Wrenn received a notification from Defendant indicating that her PII and/or PHI may have been affected by the Data Breach.

17. Plaintiff Olga Romashova is and, at all relevant times hereto, an adult who is a citizen and resident of the State of Nevada.

18. Plaintiff Romashova is a patient of Hankins. On or about March 14, 2023, Plaintiff Romashova received a notification from Defendant indicating that her PII and/or PHI may have been affected by the Data Breach.

19. Plaintiff Caroline Aurora is and, at all relevant times hereto, an adult who is a citizen and resident of the State of Nevada.

20. Plaintiff Aurora is a patient of Hankins. In or around March 2023, Plaintiff Aurora received a notification from Defendant indicating that her PII and/or PHI may have been affected by the Data

Breach.

21. Plaintiff Sarah Jefferson is and, at all relevant times hereto, an adult who is a citizen and resident of the State of Nevada.

22. Plaintiff Jefferson is a patient of Hankins. On or about November 17, 2023, Plaintiff received an email from the threat actors and became aware that her PII and/or PHI had been leaked in the Data Breach.

23. Defendant Hankins is, and at all relevant times hereto, a Nevada professional corporation with a principal place of business located in Las Vegas, Nevada. Defendant Hankins is a citizen of Nevada.

JURISDICTION AND VENUE

24. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class is a citizen of a state different than Defendant.

25. This Court has personal jurisdiction over Defendant because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District and Defendant resides in this District.

26. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

FACTUAL BACKGROUND

Hankins Collected and Stored Plaintiffs' and Class Members' PII and PHI.

27. Hankins is a plastic surgery group practice that provides the greater Las Vegas Valley "with the very best of surgical and nonsurgical care," including face, breast, body, and male plastic surgery along with non-surgical treatments including injectables and dermal fillers, skin resurfacing, skin tightening, laser hair removal, non-surgical body contouring, and skin care products.[3]

28. "At Hankins & Sohn Plastic Surgery Associates, our board certified plastic surgeons, W. Tracy Hankins, MD and Samuel M. Sohn, MD believe in patient safety, world-class results, and

[3] *Hankins Plastic Surgery Center*, https://www.hankinsplasticsurgery.com/ (last visited Sept. 15, 2023).

compassionate care. With this commitment in mind, we invite patients from around the world to experience the art and science of plastic surgery through the hands, hearts, and minds of Dr. Hankins and Dr. Sohn."[4]

29. As a condition of providing the above-described healthcare services to Plaintiffs and Class Members, Plaintiffs are informed and believe, that Hankins receives, creates, and handles PII and PHI, which includes patient names, contact information, dates of birth, Social Security Numbers, driver's license information, medical histories, consultation notes, and photos.

30. Plaintiffs and Class Members must entrust Hankins with their sensitive and confidential PII and PHI in order to receive healthcare services, and in return reasonably expected that Hankins would safeguard their highly sensitive information and keep it confidential.

31. By obtaining, collecting, and storing Plaintiffs' and Class Members' PII and PHI, Hankins assumed equitable and legal duties to safeguard and keep confidential Plaintiffs' and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

32. Even though "[t]he confidentiality, privacy, and security of information in [Defendant's] care are [its] highest priorities,"[5] Hankins nevertheless employed inadequate data security measures to protect and secure the PII and PHI patients entrusted to it, resulting in the Data Breach and the exfiltration of Plaintiffs' and Class Members' PII and PHI stored within its computer network.

Hankins Breached its Duty to Protect its Patients.

33. Hankins was well aware that the PII and PHI it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

34. Hankins also knew that a breach of its computer systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

---

[4] *About the Practice*, Hankins Plastic Surgery Center, https://www.hankinsplasticsurgery.com/about/ (last visited Sept. 15, 2023).

[5] Notice of Data Breach, *supra* note 2.

35. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, and many others.

36. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[6] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

37. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[7]

38. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[8]

39. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[9] Indeed, "[t]he IT environments of healthcare organizations are often complex and difficult to secure. Devices and software continue to be used that have reached end-of-life, as upgrading is costly and often problematic. Many healthcare providers use software solutions that have

---

[6] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[7] *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/.

[8] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Sept. 15, 2023).

[9] *The healthcare industry is at risk*, SwivelSecure https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Sept. 15, 2023).

been developed to work on specific – and now obsolete – operating systems and cannot be transferred to supported operating systems."[10]

40. Additionally, "[h]ospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[11]

41. Cybercriminals seek out PHI at a greater rate than other sources of personal information. Between 2009 and 2022, 5,150 healthcare data breaches of 500 or more individuals have been reported to Health and Human Services' Office of Civil Rights, resulting in the exposure or unauthorized disclosure of the information of 382,262,109 individuals—"[t]hat equates to more than 1.2x the population of the United States."[12]

42. Further, the rate of healthcare data breaches has been on the rise in recent years. "In 2018, healthcare data breaches of 500 or more records were being reported at a rate of around 1 per day. Fast forward 5 years and the rate has more than doubled. In 2022, an average of 1.94 healthcare data breaches of 500 or more records were reported each day."[13]

43. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[14]

44. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[15]

---

[10] Steve Alder, Editorial: *Why Do Criminals Target Medical Records*, HIPAA Journal (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records/#:~:text=Healthcare%20records%20are%20so%20valuable,credit%20cards%20in %20victims'%20names.

[11] *Id.*

[12] *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited Sept. 15, 2023).

[13] *Id.*

[14] *2022 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report (last visited Sept. 15, 2023).

[15] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.

45. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Hanins's patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

46. **Social Security Numbers**—Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique social security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

47. The Social Security Administration even warns that the process of replacing a Social Security is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.

If you receive a new Social Security Number, you should not be able to use the old number anymore.

For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[16]

48. Social Security Numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of

[16] *Identify Theft and Your Social Security Numbers*, Social Security Admin. (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

49. **Driver's License Numbers—**are highly sought after by cyber criminals on the dark web because they are unique to a specific individual and extremely sensitive. This is because a driver's license number is connected to an individual's vehicle registration, insurance policies, records on file with the DMV, places of employment, doctor's offices, government agencies, and other entities.

50. For these reasons, driver's license numbers are highly sought out by cyber criminals because they are one of the most valuable pieces of information to facilitate identity theft and fraud. This information is valuable because cyber criminals can use this information to open credit card accounts, obtain insurance policies and submit fraudulent claims, open cell phone contracts, file fraudulent tax returns, file unemployment applications, as well as obtain bank loans under a person's name.

51. Further, unlike credit or debit card numbers in a payment card data breach, which can quickly be frozen and reissued in the aftermath of a breach, the type of PII at stake here—unique driver's license numbers—cannot be easily replaced.

52. **Medical Information**—As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[17] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[18]

53. Indeed, medical records "are so valuable because they can be used to commit a multitude of crimes. Healthcare data can be used to impersonate patients to obtain expensive medical services,

---

[17] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, IDX (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[18] *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*, PriceWaterhouseCoopers, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited Sept. 15, 2023).

Medicare and Medicaid benefits, healthcare devices, and prescription medications. Healthcare records also contain the necessary information to allow fraudulent tax returns to be filed to obtain rebates."[19]

54. "In contrast to credit card numbers and other financial information, healthcare data has an incredibly long lifespan and can often be misused for long periods undetected. Credit card companies monitor for fraud and rapidly block cards and accounts if suspicious activity is detected, but misuse of healthcare data is harder to identify and can be misused in many ways before any malicious activity is detected. During that time, criminals can run up huge debts – far more than is usually possible with stolen credit card information."[20]

55. According to Experian:

Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.

ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.

Victims of healthcare data breaches may also find themselves being denied care, coverage, or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[21]

56. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being

---

[19] Alder, *supra* note 10.

[20] *Id.*

[21] Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[22]

57. Based on the value of its patients' PII and PHI to cybercriminals, Hankins knew or should have known, the importance of safeguarding the PII and PHI entrusted to it and of the foreseeable consequences if its data security systems were breached. Hankins failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

58. Plastic surgeons, including Defendant, routinely collect, handle and maintain PII and PHI as part of their practice.

59. As such, there are standards that plastic surgeons, including Defendant should have followed when collecting, handling and maintaining PII and PHI, such as the PII and PHI that is the subject of this matter.

Hankins Breached its Duty to Protect Patient PII and PHI.

60. On or about March 14, 2023, Plaintiffs received email notifications from Defendant, informing them that a threat actor had stolen data from Hankin's computer network. The email notice further informed Plaintiffs that the threat actor threatened to reach out to Defendant's patients about the stolen information, *i.e.*, the threat actor threatened to use the stolen information to extort Plaintiffs and other of Defendant's patients.

61. Despite the threat actor stealing information from Defendant's computer network and threatening to extort it patients, Defendant did not offer Plaintiffs or Class members identity theft protection services in its March 14,2023 email notice. Instead, Defendant simply advised Plaintiffs and class members to "lock down" their social media profiles and monitor their accounts.

62. On or about April 3, 2023, Defendant began mailing data breach notifications to impacted patients.

63. According to Hankins, on or about February 23, 2023, Defendant discovered suspicious activity relating to allegations made by a threat actor that data was stolen from its network.

---

[22] U.S. Gov't Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited Sept. 15, 2023).

64. Upon discovering the suspicious activity, Hankins investigated the claims of the threat actor and claims to have determined the nature and scope of the activity and what information was compromised. Hankins' investigation revealed that at some point prior to February 23, 2023, the threat actor had exfiltrated certain files from Hankins' computer network.

65. A wide variety of patient PII and PHI was compromised during the data breach, including but not limited to patient names, contact information, dates of birth, Social Security Numbers, driver's license information, medical histories, consultation notes, and photos.

66. Upon information and belief, following the Data Breach, the threat actor held the stolen information for ransom and demanded that Hankins pay. After Hankins refused to pay the ransom, the threat actor then began demanding ransom payments from individual patients. The threat actor warned patients that if they refused to pay the ransom, the threat actor would send patients' stolen PII and PHI to their friends, families, and colleagues.

67. Following the threat actor's individual ransom attempts directed at Defendant's patients, the threat actor published the stolen information on its leak site(s). On the leak site(s), the threat actor claimed to have downloaded everything from Defendant's plastic surgery clinic's network, including documents and pre- and post-op photos pertaining to more than 10,000 of Defendant's patients. The stolen patient information posted on the leak site(s) includes 131 patients' nude photos, names, email addresses, and phone numbers.[23] The number of patients included on the leak site(s) appears to increase as time goes on.

68. The threat actor further advertised that patients could have their information removed from the leak site if they provided a review about Hankins. However, the threat actor made clear that they would not delete any of the stolen information and the leak site—the threat actor would only delete the website and stolen patient information if and when Hankins paid a ransom.

[23] Due to the sensitive nature of the information displayed on the leak site, Plaintiffs have not provided a link to the leak site out of respect for individuals' privacy.

69. According to information provided to the Indiana Attorney General, the Data Breach impacted more than 12,000 individuals.[24]

70. Plaintiffs are informed and believe that the Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures in order to protect its patients' PII and PHI.

FTC Guidelines Prohibit Hankins from Engaging in Unfair or Deceptive Acts or Practices.

71. Hankins is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act

72. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[25]

73. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[26]

74. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[27]

---

[24] *2023 Data Breach Year to Date Report*, Office of the Indiana Attorney General https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/files/2023-Data-Breach-Year-to-Date-Report.pdf (last visited Sept. 15, 2023).

[25] *Start with Security: A Guide for Business*, Fed. Trade Comm'n, https://www.ftc.gov/business-guidance/resources/start-security-guide-business (last visited Sept. 15, 2023).

[26] *Protecting Personal Information: A Guide for Business*, Fed. Trade Comm'n, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Sept. 15, 2023).

[27] *Id.*

75. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

76. Upon information and belief Hankins failed to properly implement one or more of the basic data security practices recommended by the FTC. Hankins' failure to employ reasonable and appropriate data security measures to protect against unauthorized access to patients' PII and/or PHI constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

77. Hankins was at all times fully aware of its obligations to protect the PII and/or PHI of patients because of its position as a healthcare provider, which gave it direct access to reams of PII and/or PHI. Hankins was also aware of the significant repercussions that would result from its failure to do so.

Hankins is Obligated Under HIPAA to Safeguard Patient PHI.

78. Hankins is required by the Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. § 1302d, *et seq*. to safeguard patient PHI.

79. Hankins is an entity covered by under HIPAA, which sets minimum federal standards for privacy and security of PHI.

80. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

81. Under 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."

82. Under C.F.R. § 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either (a) identifies

the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

83. HIPAA requires Hankins to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et seq*.

84. The Department of Health and Human Services Office for Civil Rights further recommends the following data security measures a regulated entity such as Hankins should implement to protect against some of the more common, and often successful, cyber-attack techniques:

a. Regulated entities should implement security awareness and training for all workforce members and that the training programs should be ongoing, and evolving to be flexible to educate the workforce on new and current cybersecurity treats and how to respond;

b. Regulated entities should implement technologies that examine and verify that received emails do not originate from known malicious site, scan web links or attachments included in emails for potential threats, and impeded or deny the introduction of malware that may attempt to access PHI;

c. Regulated entities should mitigate known data security vulnerabilities by patching or upgrading vulnerable technology infrastructure, by upgrading or replacing obsolete and/or unsupported applications and devices, or by implementing safeguards to mitigate known vulnerabilities until an upgrade or replacement can occur;

d. Regulated entities should implement security management processes to prevent, detect, contain, and correct security violations, including conducting risk assessments to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI; and

e. Regulated entities should implement strong cyber security practices by requiring strong passwords rules and multifactor identification.[28]

85. Upon information and belief, Hankins failed to implement one or more of the recommended data security measures.

86. While HIPAA permits healthcare providers and their business associates to disclose PHI to third parties under certain circumstances, HIPAA does not permit healthcare providers to disclose PHI to cybercriminals, nor did Plaintiffs or the Class Members consent to the disclosure of their PHI to cybercriminals.

87. As such, Defendant is required under HIPAA to maintain the strictest confidentiality of Plaintiffs' and Class Members' PHI that they acquire, receive, and collect, and Defendant is further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

88. Given the application of HIPAA to Hankins, and that Plaintiffs and Class Members directly or indirectly entrusted their PHI to Defendant in order to receive healthcare services from Hankins, Plaintiffs and Class Members reasonably expected that Defendant would safeguard their highly sensitive information and keep their PHI confidential.

Plaintiffs' Experiences.

Plaintiff Tausinga

89. Plaintiff Tausinga was a patient of Defendant. On or about March 14, 2023, Plaintiff Tausinga received an email notification from Defendant informing her that the PII and PHI she provided to Hankins was compromised in the Data Breach.

90. Since the announcement of the Data Breach, Plaintiff Tausinga has experienced fraud. By March 28, 2023, the threat actor was threatening Plaintiff Tausinga through the WhatsApp mobile application to distribute her PII and PHI to her friends, colleagues, and neighbors, unless she paid a ransom

[28] *OCR Quarter 1 2022 Cybersecurity Newsletter*, U.S. Dept't of Health & Human Services (mar. 17, 2023), https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-first-quarter-2022/index.html.

to the threat actor directly. Plaintiff Tausinga later notified Hankins of the communication she received from the threat actor.

91. When Plaintiff Tausinga refused to pay the threat actor's demands, the threat actor shared her consultation photos with friends, colleagues, and neighbors. Hankins took no steps to prevent the release of the PII and/or PHI to Plaintiff Tausinga's friends, colleagues, and neighbors. As a direct and proximate result of Hankins' failure to safeguard her PII and/or PHI, Plaintiff Tausinga has been subjected to extortion and the mental anguish of having her sensitive PII and PHI exposed to her friends, colleagues, and neighbors.

92. Since the announcement of the Data Breach, Plaintiff Tausinga has been required to spend her valuable time and resources (1) mitigating the risk of the fraud she has experienced and (2) in an effort to detect and prevent any misuses of her PII and PHI. Plaintiff Tausinga would not have to undergo such time-consuming efforts but for the Data Breach.

93. As a direct and proximate result of the Data Breach, Plaintiff Tausinga has been and will continue to be at a heightened risk for fraud and identity theft and its attendant damages for years to come. Such a risk is real and certainly impending, and is not speculative, given the highly sensitive nature of the PII and PHI compromised in the Data Breach, and that this information was already illegally used by the threat actor after the Data Breach to extort Plaintiff Tausinga.

Plaintiff Wrenn

94. Plaintiff Wrenn was a patient of Defendant. On or about March 24, 2023, photographs and information possessed and stored by Defendant, including images of Plaintiff Wrenn's medical treatment and of her medical charts, were made public via e-mails sent to Plaintiff Wrenn's employer and others.

95. Since the announcement of the Data Breach, and as recently as September 2023, Plaintiff Wrenn has experienced fraud. On September 3, 2023, the threat actor utilized the Proton electronic mail service to contract Plaintiff Wrenn, threatening to distribute her PII and PHI to her friends, colleagues, and neighbors. Plaintiff Wrenn's image, birthdate, email address and phone number have been also added to the threat actor's leak site(s).

96. In addition, Plaintiff Wrenn's PII and PHI compromised in the Data Breach has been disseminated to her friends, colleagues, neighbors, and others. Plaintiff Wrenn learned of and/or was made

aware of the dissemination of her PII and PHI after being told of such dissemination by her friends, colleagues, and neighbors. Plaintiff Wrenn also recently learned of an Instagram account as late as September 8, 2023, which is continuing to disseminate Wrenn's PII and PHI.

97. As a direct and proximate result of Hankins' failure to safeguard her PII and/or PHI, Plaintiff Wrenn has been subjected to extortion and the mental anguish of having her sensitive PII and PHI exposed to her friends, colleagues, and neighbors.

98. Since the announcement of the Data Breach, Plaintiff Wrenn has been required to spend her valuable time and resources (1) mitigating the risk of the fraud she has experienced and (2) in an effort to detect and prevent any misuses of her PII and PHI. Plaintiff Wrenn would not have to undergo such time-consuming efforts but for the Data Breach.

99. As a direct and proximate result of the Data Breach, Plaintiff Wrenn's sensitive PII and PHI has been exposed and Wrenn will continue to be at a heightened risk for fraud and identity theft and its attendant damages for years to come. Such a risk is real and certainly impending, and is not speculative, given the highly sensitive nature of the PII and PHI compromised in the Data Breach, and that this information was already illegally used by the threat actor after the Data Breach to extort Plaintiff Wrenn.

Plaintiff Romashova

100. Plaintiff Romashova is a patient of Defendant. On or about March 14, 2023, Plaintiff Romashova received an email notification from Defendant informing her that the PII and PHI she provided to Hankins was compromised in the Data Breach, including her name, Social Security Number, date of birth, and address.

101. Since the announcement of the Data Breach, Plaintiff Romashova has experienced fraud. On July 10, 2023, she received an email from the threat actor stating that they would release her photos and personal information stolen from Hankins. On July 12, 2023, she received another email from the threat actor including a link to a website where nude pre- and post-operation photographs of Plaintiff Romashova and other patients could be found, along with their personal information. Plaintiff Romashova was told by the threat actor that they would remove her information if she paid them $800.

102. When Plaintiff Romashova reached out to Hankins, Defendant told her to submit a claim to the FBI, which she did on July 10, 2023.

103. As a direct and proximate result of Hankins' failure to safeguard her PII and/or PHI, Plaintiff Romashova has been subjected to extortion and the mental anguish of having her sensitive PII and PHI exposed to the public.

104. Since the announcement of the Data Breach, Plaintiff Romashova has been required to spend her valuable time and resources (1) mitigating the risk of the fraud she has experienced and (2) attempting to detect and prevent any misuses of her PII and PHI. Plaintiff Romashova would not have to undergo such time-consuming efforts but for the Data Breach.

105. As a direct and proximate result of the Data Breach, Plaintiff Romashova has been and will continue to be at a heightened risk for fraud and identity theft and its attendant damages for years to come. Such a risk is real and certainly impending, and is not speculative, given the highly sensitive nature of the PII and PHI compromised in the Data Breach.

Plaintiff Aurora

106. Plaintiff Aurora was a patient of Defendant. In or around March 2023, Plaintiff Aurora was notified by Hankins of the Data Breach involving confidential and compromising PHI of Plaintiff, including her name, Social Security Number, date of birth, address, financial account information, and sensitive photographs.

107. Since the announcement of the Data Breach, Plaintiff Aurora has been required to spend her valuable time and resources (1) mitigating the risk of the fraud she has experience and (2) in an effort to detect and prevent any misuses of her PII and PHI. Plaintiff Aurora would not have to undergo such time-consuming efforts but for the Data Breach.

108. As a direct and proximate result of the Data Breach, Plaintiff Aurora has been and will continue to be at a heightened risk for fraud and identity theft and its attendant damages for years to come. Such a risk is real and certainly impending, and is not speculative, given the highly sensitive nature of the PII and PHI compromised in the Data Breach, and that this information was already illegally accessed by the threat actor after the Data Breach.

109. As a direct and proximate result of the Data Breach, Plaintiff Aurora has continuously suffered fear, anxiety, and stress due to the present and future risk of being a victim of identity fraud and extortion but for the Data Breach.

Plaintiff Jefferson

110. Plaintiff Jefferson was a patient of Defendant. On or about November 17, 2023, Plaintiff Jefferson received an email notification from the threat actors stating that her PII, PHI, and photographs were posted on website.

111. Plaintiff Jefferson followed the website link provided in the email and confirmed that her private photos and sensitive information were posted to the website.

112. Since the announcement of the Data Breach, Plaintiff Jefferson has been required to spend her valuable time and resources (1) mitigating the risk of the fraud she has experienced and (2) in an effort to detect and prevent any misuses of her PII and PHI. Plaintiff Wrenn would not have to undergo such time-consuming efforts but for the Data Breach.

113. As a direct and proximate result of the Data Breach, Plaintiff Jefferson has been and will continue to be at a heightened risk for fraud and identity theft and its attendant damages for years to come. Such a risk is real and certainly impending, and is not speculative, given the highly sensitive nature of the PII and PHI compromised in the Data Breach, and that this information was already illegally accessed by the threat actor after the Data Breach.

114. As a direct and proximate result of the Data Breach, Plaintiff Jefferson has continuously suffered fear, anxiety, and stress due to the present and future risk of being a victim of identity fraud and extortion but for the Data Breach.

Plaintiffs and Class Members Have Suffered Damages.

115. For the reasons mentioned above, Hankins' conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class Members significant injuries and harm in several ways, including actual fraud as well as substantial and imminent risk of identity theft and fraud. Plaintiffs and Class Members must immediately devote time, energy, and money to: (1) closely monitor their medical statements, bills, records, and credit and financial accounts; (2) change login and password information on any sensitive

account even more frequently than they already do; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering, spear phishing, or extortion attacks; and (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

116. Indeed, the threat actor stole PII and PHI from Hankins with the specific intent to use it for illicit purposes as demonstrated by the threat actor's extortion attempts directed at Plaintiffs and Class Members, along with the sharing of Plaintiffs' and Class Members' PII and PHI with families, friends, and colleagues and posting the same on its leak site(s). These facts distinguish this case from other data breaches that involve only a speculative risk of harm.

117. Once PII and PHI are exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Hankins' conduct. Further, the value of Plaintiffs' and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

118. As a result of Hankins' failures, Plaintiffs and Class Members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of the Data Breach. Those impacted are under heightened and prolonged anxiety and fear, as they will be at risk of falling victim to cybercrimes for years to come.

119. With respect to healthcare breaches, another study found "the majority [70 percent] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[29]

120. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[30]

---

[29] Jessica David, *70% of Data Involved in Healthcare Breaches Increases Risk of Fraud*, HEALTHITSECURITY, https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud (last visited Sept. 15, 2023).

[30] *Id.*

121. Indeed, PII and PHI are valuable commodities to identity thieves and once they have been compromised, criminals will use them and trade the information on the cyber black market for years thereafter. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security Numbers, and bank account information, complete with account routing numbers can fetch up to $1,200 to $1,300 each on the black market.[31] According to a report released by the FBI's cyber division, criminals can sell healthcare records for 50 times the price of stolen Social Security Numbers or credit card numbers.[32]

122. The reality is that cybercriminals seek nefarious outcomes from a data breach and "stolen health data can be used to carry out a variety of crimes."[33]

123. Health information in particular is likely to be used in detrimental ways, by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[34]

124. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[35]

125. Plaintiffs and Class Members are also at a continued risk because their information remains in Hankins' systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Hankins fails to undertake the necessary and appropriate security and training measures to protect its patients' PII and PHI.

---

[31] Adam Greenberg, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC Media, (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[32] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[33] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH, (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

[34] *Id.*

[35] *The Potential Damages and Consequences of Medical Identity theft and Healthcare Data Breaches*, EXPERIAN, https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited Sept. 15, 2023).

126. Plaintiffs and Class Members have lost the benefit of their bargains. Plaintiffs and Class Members entered into agreements with and provided payment to Hankins under the reasonable but mistaken belief that it would reasonably and adequately protect their PII and PHI. Plaintiffs and Class Members would not have entered into such agreements and would not have paid Hankins the amount that they paid had they known that Hankins would not reasonably and adequately protect their PII and PHI. Plaintiffs and Class Members have thus suffered actual damages in an amount at least equal to the difference in value between the healthcare services that include reasonable and adequate data security that they bargained for, and the healthcare services that do not, which they actually received.

127. Plaintiffs and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers and their families, friends, and colleagues.

CLASS ACTION ALLEGATIONS

128. Plaintiffs bring this class action on behalf of themselves and all others who are similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

129. Plaintiffs seek to represent the following Class of persons defined as follows:

> All individuals in the United States whose PII and/or PHI was compromised in the Hankins Data Breach which occurred on or about February 23, 2023 (the "Class").

130. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

131. This proposed class definition is based on the information available to Plaintiffs at this time. Plaintiffs may modify the class definition in an amended pleading or when they move for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

132. **Numerosity:** The members of the Class are so numerous that the joinder of all members is impractical. Plaintiffs are informed and believe, and thereon allege, that there are at minimum, thousands of members of the Class described above. The exact size of the Class and the identities of the individual

members are identifiable through Hankins' records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes approximately 12,500 individuals.

133. **Commonality:** This action involved questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether Hankins had a duty to protect the PII and PHI of Plaintiffs and Class Members;

b. Whether Hankins was negligent in collecting and storing Plaintiffs' and Class Members' PII and PHI, and breached its duties thereby;

c. Whether Hankins entered contracts implied in fact with Plaintiffs and the Class;

d. Whether Hankins breached those contracts by failing to adequately safeguard Plaintiffs' and Class Members' PII and PHI;

e. Whether Hankins was unjust enriched to the detriment of Plaintiffs and the Class;

f. Whether Hankins' conduct is violative of the Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600;

g. Whether Hankins' conduct constitutes professional negligence;

h. Whether Plaintiffs and Class Members are entitled to damages as a result of Hankins' wrongful conduct; and

i. Whether Plaintiffs and Class Members are entitled to restitution as a result of Hankins' wrongful conduct.

134. **Typicality:** Plaintiffs' claims are typical of the claims of Class Members. Plaintiffs' and Class Members' claims are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiffs and Class Members were all patients of Hankins, each having their PII and PHI exposed and/or accessed by an unauthorized third party.

135. **Adequacy:** Plaintiffs are adequate representatives of the Class. Plaintiffs will fairly, adequately, and vigorously represent and protect the interests of the Class Members and have no interests antagonistic to the Class Members. In addition, Plaintiffs have retained counsel who are competent and

experienced in the prosecution of class action litigation. The claims of Plaintiffs and the Class Members are substantially identical as explained above.

136. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all Class members is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

137. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiffs and each member of the Class. If Defendant breached its duty to Plaintiffs and Class Members, then Plaintiffs and each Class member suffered damages by that conduct.

138. **Injunctive Relief:** Defendant has acted and/or refused to act on grounds that generally apply to the Class making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

139. **Ascertainability:** Class Members are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Hankins' books and records.

FIRST CAUSE OF ACTION
NEGLIGENCE
(Plaintiffs on Behalf of Class)

140. Plaintiffs restate and reallege all proceeding allegations above as if fully set forth herein.

141. Hankins owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and/or PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty including, among other things: (a) designing, maintaining, and testing its security systems to ensure that Plaintiffs' and Class Members' PII and/or PHI in Hankins' possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely

manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

142. Hankins' duty to use reasonable care arose from several sources, including but not limited to those described below.

143. Hankins had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing valuable PII/PHI that is routinely targeted by cyber-criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

144. Hankins' duty also arose from Defendant's special relationship with its patients as a result of its position as a healthcare provider. Hankins holds itself out as a trusted provider of healthcare services, and thereby assumes a duty to reasonably protect its patients' information. Indeed, Hankins who directly provides healthcare services, was in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

145. Further, Hankins duty arose from various statutes requiring Defendant to implement reasonable data security measures, including but not limited to, Section 5 of the FTC Act, HIPAA, and Nev. Rev. Stat. § 603A.210.

146. Hankins' is subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs and Defendant and Class Members. The sources of Hankins' duty are identified above.

147. Hankins' violation of Section 5 of the FTC Act, HIPAA, and stat data security statutes constitutes negligence *per se* for purposes of establish the duty and breach elements of Plaintiffs' negligence claim. Those statutes were designed to protect a group to which Plaintiffs and Class Members belong and to prevent the type of harm that resulted from the Data Breach.

148. Hankins' conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Hankins conduct included its failure to adequately restrict access to its computer networks that held patients' PII and PHI.

149. Hankins knew or should have known of the inherent risk in collecting and storing massive amounts of PII, the importance of implementing adequate data security measures to protect that PII and PHI, and the frequency of cyberattacks such as the Data Breach in the healthcare sector.

150. Defendant breached the duties owed to Plaintiffs and Class Members and thus was negligent. Defendant breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII and/or PHI of Plaintiffs and Class Members; (b) detect the Data Breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose that Plaintiffs' and Class Members' PII and/or PHI in Defendant's possession had been or was reasonably believed to have been, stolen or compromised.

151. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, their PII and/or PHI would not have been compromised.

152. As a direct and proximate result of Hankins' negligence, Plaintiffs and Class Members have suffered injuries, including: (i) actual identity theft; (ii) the loss of the opportunity how their PII and/or PHI is used; (iii) the compromise, publication, and/or theft of their PII and/or PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and/or PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII and/or PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII and/or PHI in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and/or PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

153. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, damages in an amount to be proven at trial.

/ / /

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(Plaintiffs on behalf of the Class)

154. Plaintiffs restate and reallege all preceding allegations set forth above as if fully alleged herein.

155. Plaintiffs bring this claim individually and on behalf of the Class.

156. When Plaintiffs and Class Members provided their PII and PHI to Hankins in exchange for healthcare services, they entered into implied contracts with Defendant, under which Hankins agreed to take reasonable steps to protect Plaintiffs' and Class Members' PII and PHI.

157. Hankins solicited and invited Plaintiffs and Class Members to provide their PII and PHI, including their names, addresses, dates of birth, phone numbers, email addresses, various forms of identification, and medical information, as part of Defendant's provision of healthcare services. Plaintiffs and Class Members accepted Hankins' offers and provided their PII and PHI to Defendant.

158. When entering into implied contracts, Plaintiffs and Class Members reasonably believed and expected that Hankins employed adequate data security measures to safeguard their PII and PHI. Implicit in the agreement between Plaintiffs and Class Members and Defendant to provide PII and/or PHI, was the latter's obligation to: (a) use such PII and/or PHI for business purposes only, (b) take reasonable steps to safeguard that PII and/or PHI, (c) to prevent unauthorized disclosures of the PII and/or PHI, (d) to provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII and/or PHI, (e) to reasonably safeguard and protect the PII and/or PHI of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) to retain the PII and/or PHI only under conditions that kept such information secure and confidential.

159. Plaintiffs are informed and believe that in Defendant's written privacy policies, Hankins expressly promised Plaintiffs and Class Members that Defendant would only disclose PII and/or PHI under certain circumstances, none of which relate to the Data Breach. Plaintiffs and Class Members paid money to Hankins in the form of co-pays and other similar payments in order to receive healthcare services. Plaintiffs and Class Members reasonably believed and expected that Hankins would use part of those funds to obtain adequate data security. Hankins failed to do so.

160. Plaintiffs and Class Members would not have provided their PII and PHI to Defendant had

they known that Hankins would not safeguard their PII and PHI as promised.

161. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Hankins.

162. Hankins breached its implied contracts with Plaintiffs and Class Members by failing to safeguard Plaintiffs' and Class Members' PII and PHI.

163. The losses and damages Plaintiffs sustained, include, but are not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and/or PHI is used; (iii) the compromise, publication, and/or theft of their PII and/or PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and/or PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII and/or PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII and/or PHI in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and/or PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

164. As a direct and proximate result of Hankins' breach of contract, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(Plaintiffs on Behalf of the Class)

165. Plaintiffs restate and reallege all proceeding factual allegations above as if fully set forth herein.

166. Plaintiffs bring this claim individually and on behalf of the Class in the alternative to Plaintiffs' Implied Contract claim.

167. Upon information and belief, Hankins funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and Class Members.

168. As such, a portion of the payments made by or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Hankins.

169. Plaintiffs and Class Members conferred a monetary benefit on Hankins. Specifically, they purchased goods and services from Defendant and in so doing provided Defendant with their PII and/or PHI. In exchange, Plaintiffs and Class Members should have received from Hankins the goods and services that were the subject of the transaction and have their PII and/or PHI protected with adequate data security.

170. Hankins knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Hankins profited from these transactions and used the PII and/or PHI of Plaintiffs and Class Members for business purposes, including very personal photographs taken of Plaintiffs and Class Members.

171. In particular, Hankins enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the Data Breach, Hankins instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

172. Under the principles of equity and good conscience, Hankins should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

173. Hankins failed to secure Plaintiffs' and Class Members' PII and/or PHI and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

174. Hankins acquired the PII and/or PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

175. If Plaintiffs and Class Members knew that Defendant had not secured their PII and/or PHI, they would not have agreed to provide their PII and/or PHI to Hankins, including very personal photographs taken of Plaintiffs and Class Members.

176. Plaintiffs and Class Members have no adequate remedy at law.

177. As a direct and proximate result of Hankins wrongful conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and/or PHI is used; (iii) the compromise, publication, and/or theft of their PII and/or PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and/or PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII and/or PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII and/or PHI in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and/or PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

178. As a direct and proximate result of Hankins' conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

179. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services, or Defendant should be compelled to place a percentage of all future profits into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, designed to represent the value obtained by the use of the inadequately secured PII and/or PHI compromised as a result of the Data Breach.

FOURTH CAUSE OF ACTION
VIOLATION OF THE NEVADA CONSUMER FRAUD ACT
Nev. Rev. Stat. § 41.600
(Plaintiffs on Behalf of the Class)

180. Plaintiffs restate and reallege all proceeding factual allegations above as if fully set forth herein.

181. The Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600 states in relevant part:

182. An action may be brough by any person who is a victim of consumer fraud.

183. As used in this section, "consumer fraud" means: . . . A deceptive trade practice defined in NRS 598.0915 to 598.0225, inclusive.

Nev. Rev. Stat. § 41.600(1) & (2)(e).

184. In turn, Nev. Rev. Stat. § 598.0923(2) provides that "[a] person engages in a 'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly . . . [f]ails to disclose a material fact in connection with the sale or lease of goods or services." *Id.* Hankins violated this provision because it failed to disclose the material fact that its data security measures were inadequate to reasonably safeguard its patients' PII and PHI. This is true because, among other things, Hankins was aware that the healthcare sector is a frequent target of cyberattacks such as the Data Breach. Hankins knew or should have known that that its data security measures were insufficient to guard against attacks such as the Data Breach. Hankins and knowledge of the facts that constituted the omission. Hankins could have and should have made a proper disclosure when accepting new patients, while providing healthcare services, or by any other means reasonably calculated to inform customers of its inadequate data security measures.

185. Further, Nev. Rev. Stat. § 598.0923(3) provides that "[a] person engages in a 'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly . . . [v]iolates a state or federal statute or regulation relating to the sale or lease of goods or services." *Id.* Hankins violated this provision for several reasons, each of which serves as an independent basis for violating Nev. Rev. Stat. § 598.0923(3).

186. First, Hankins breached its duty under Nev. Rev. Stat. § 603A.210, which requires any data collector "that maintains records which contain personal information" of Nevada residents to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, . . . use, modification or disclosure." *Id.* Hankins is a "data collector" as defined by Nev. Rev. Stat. § 603A.030. Hankins failed to implement such reasonable security measures, as shown by a system-wide breach of its computer systems during which a threat actor exfiltrated patient PII and PHI that was later used to extort Plaintiffs and Class Members. Hankins' violation of this statute was done knowingly for

the purposes of Nev. Rev. Stat. § 598.0923(3) because Hankins knew or should have known that the healthcare sector is a frequent target of cyberattacks such as the Data Breach. Hanins knew or should have known that its data security measures were inadequate to protect against cyberattacks such as the Data Breach.

187. Second, Hankins violated Section 5 of the FTC Act and HIPAA, as alleged above. Hankins knew or should have known that its data security measures were inadequate, violated Section 5 of the FTC Act, violated HIPAA, failed to adhere to the FTC's data security guidance, and failed to adhere to HHS's data security guidance. This is true because Hankins was well aware that the healthcare sector is a frequent target of cyberattacks such as the Data Breach and both the FTC and HHS have recommended various data security measures that companies such as Defendant could have implemented to mitigate the risk of a Data Breach. Hankins chose not to follow such guidance and knew or should have known that its data security measures were inadequate to guard against cyberattacks such as the Data Breach. Hankins had knowledge of the facts that constituted the violation. Hankins' violation of Section 5 of the FTC Act and HIPAA serve as a separate actional basis for purposes of violating Nev. Rev. Stat. § 598.0923(3).

188. Hankins engaged in an unfair practice by engaging in conduct that is contrary to public policy, unscrupulous, and caused injury to Plaintiffs and Class Members.

189. Plaintiff and members of the Class were denied a benefit conferred on them by the Nevada legislature.

190. As a direct and proximate result of the foregoing, Plaintiffs and Class Members have suffered injuries including, but not limited to actual damages, and in being denied a benefit conferred on them by the Nevada legislature.

191. As a result of these violations, Plaintiffs and Class Members are entitled to an award of actual damages, equitable injunctive relief requiring Defendant to implement adequate data security measures, as well as an award of reasonable attorney's fees and costs. Nev. Rev. Stat. § 41.600(3).

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(Plaintiffs on behalf of the Class)

192. Plaintiffs restate and reallege all preceding allegations set forth above as if fully alleged herein.

193. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et. seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Consolidated Amended Class Action Complaint.

194. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII and PHI and whether Hankins is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII and PHI. Plaintiffs allege that Defendant's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their PII and PHI and remains at imminent risk that further compromises of their PII and/or PHI will occur in the future.

195. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that, among other things:

a. Hankins owed a legal duty to secure members' PII and PHI under the common law, Section 5 of the FTC Act, HIPAA, and state data security laws; and

b. Hankins breached and continues to breach this legal duty by failing to employ reasonable measures to secure patients' PII and PHI.

196. This Court also should issue corresponding prospective injunctive relief requiring Hankins to employ adequate security protocols consistent with law and industry standards to protect members' PII and PHI.

197. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Hankins. The risk of another such breach is real, immediate, and substantial. If another breach at Hankins occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

198. The hardship to Plaintiffs and Class Members if an injunction is not issued exceeds the hardship to Hankins if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Hankins of complying with an injunction by

employing reasonable prospective data security measures is relatively minimal, and Hankins has a pre-existing legal obligation to employ such measures.

199. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Hankins, thus eliminating the additional injuries that would result to Plaintiffs, Class Members, and consumers whose confidential information would be further compromised.

SIXTH CAUSE OF ACTION
NEGLIGENT MISREPRESENTATION
(Plaintiffs on behalf of the Class)

200. Plaintiffs restate and reallege all preceding allegations set forth above as if fully alleged herein.

201. Nevada has adopted the Restatement (Second) of Torts § 551 (1977), which imposes liability for negligent misrepresentations based on omissions. Section 551, titled "Liability for Nondisclosure," states:

> One who fails to disclose to another a fact that he knows may justifiably induce the other to act or refrain from acting in a business transaction is subject to the same liability to the other as though he had represented the nonexistence of the matter that he has failed to disclose, if . . . he is under a duty to the other to exercise reasonable care to disclose the matter in question.

202. As a healthcare provider, and a recipient of its patients' PII and PHI, Defendant has a special relationship with its patients, including Plaintiffs and members of the Class.

203. Because of that special relationship, Hankins was provided with and stored private and valuable PII and PHI related to Plaintiffs and the Class. Plaintiffs and Class Members were entitled to expect that the PII and PHI entrusted to Hankins would remain confidential while in Hankins' possession.

204. Despite this special relationship, Hankins failed to disclose to Plaintiffs and Class Members that it did not employ reasonable data security safeguards to protect patients' PII and PHI.

205. Hankins's omissions were made for the guidance of patients in their transactions with Hankins.

206. Hankins failed to disclose facts that Hankins knew may justifiably induce patients to act or refrain from acting in their decision to engage with Hankins to provide them with healthcare services.

207. Hankins' omissions were made in the course of Hankin' provision of healthcare services to Plaintiffs and Class members.

208. Hankins had a duty to speak regarding the inadequacy of its data security practices and its inability to reasonably protect patients' PII and PHI.

209. Hankins knew or should have known that its data security practices were deficient. This is true because, among other things, Hankins was aware that the healthcare industry was a frequent target of sophisticated cyberattacks. Hankins knew or should have known that its data security practices were insufficient to guard against those attacks.

210. Hankins was in a special relationship with, or relationship of trust and confidence relative to, its patients. Hankins was in an exclusive position to ensure that its safeguards were sufficient to protect against the foreseeable risk that a data breach could occur. Hankins was also in exclusive possession of the knowledge that its data security processes and procedures were inadequate to safeguard patients' PII and PHI.

211. Hankins' omissions were material given the sensitivity of the PII and PHI maintained by Hankins and the gravity of the harm that could result from theft of the PII and PHI.

212. Data security was an important part of the substance of the transactions between Hankins and its patients.

213. Hankins knew or should have known that patients would enter into the provision of healthcare services under a mistake as to facts basic to the transactions. Because of the relationship between the parties, patients would reasonably expect a disclosure of the basic facts regarding Hankins' inadequate data security.

214. Had Hankins disclosed to Plaintiffs and Class Members that its systems were not secure and thus were vulnerable to attack, Plaintiffs and Class Members would not have entrusted their PII and PHI to Hankins.

215. Hankins should have made a proper disclosure to patients when accepting patient information, during the initial consultant, or by any other means reasonably calculated to inform patients of its inadequate data security.

/ / /

216. In addition to its omissions, Hankins is also liable for its implied misrepresentations. Hankins required patients to provide their PII and/or PHI during the appointment, consultation and/or check-in process. In doing so, Hankins made implied or implicit representations that it employed reasonable data security practices to protect patients' PII and PHI. By virtue of accepting Plaintiffs' and Class Members' PII and/or PHI during the appointment, consultation and/or check-in process, Hankins implicitly represented that its data security processes were sufficient to reasonably safeguard the PII and/or PHI patients entrusted to Defendant. This constituted a negligent misrepresentation.

217. Hankins failed to exercise reasonable care or competence in communicating its omissions and misrepresentations.

218. As a direct and proximate result of Hankins' omissions and misrepresentations, Plaintiffs and Class Members suffered the various types of damages alleged herein.

219. Plaintiffs and Class Members are entitled to all forms of monetary compensation and injunctive relief set forth herein.

SEVENTH CAUSE OF ACTION
PROFESSIONAL NEGLIGENCE
(Plaintiffs on behalf of the Class)

220. Plaintiffs restate and reallege all proceeding allegations set forth above as if fully alleged herein.

221. NRS 41A.015 fixes a standard of care for a provider of health care and defines "professional negligence" as "the failure of a provider of health care, in rendering services, to use the reasonable care, skill or knowledge ordinarily used under similar circumstances by similarly trained and experienced providers of health care."

222. Plaintiffs sought medical treatment from Hankins in their Las Vegas, NV and/or Henderson, NV office, and received medical care in the form of consultations, surgery, and treatment plans. Thus, a doctor-patient relationship existed between Plaintiffs and Hankins.

223. Hankins owed a duty to Plaintiffs to exercise reasonable care in rendering medical services and related treatment. Hankins' duty to use reasonable care arose from several sources, including but not limited to those described herein.

224. Hankins obtained Plaintiffs' PHI and personal information in the course of rendering services to them, including, but not limited to, names, Social Security Numbers, addresses, phone numbers, and financial information.

225. Hankins also took photographs of Plaintiffs while rendering services to them—including, but not limited to, nonconsensual, medically unnecessary photographs showing Plaintiffs' faces and other identifying information—without Plaintiffs' knowledge or consent.

226. Providers of health care like Hankins are required to use reasonable care in obtaining patient consent to take and store photographs, and they are required to use reasonable care when photographing patients. Particularly, cosmetic surgery providers are obligated to obtain patient consent prior to taking and storing photographs of a patient. Further, they are obligated to use care when photographing a patient's body to prevent the identification of the patient via the photograph(s) maintained by the health care providers.

227. Providers of health care like Hankins are required to follow the representations they make to their patients, especially when they are made in order to obtain their consent.

228. Hankins made certain representations to their patients, including Plaintiffs, in order to obtain their consent to be photographed.

229. These representations included but were not limited to Plaintiffs' consent to be photographed being contingent on Plaintiffs' identity not being revealed by the photographs.

230. The American Society of Plastic Surgeons provides guidelines for photographing plastic-surgery patients. These guidelines include explicit instructions that the photographs of patients receiving breast augmentation procedures should not include the patient's face, including other guidelines. Cosmetic surgery providers are also aware that third parties are interested in obtaining patients' private data and photographs of patients.

231. NRS 49.225 grants Plaintiffs a statutorily protected privilege to keep their private medical information confidential. Both federal and state law recognize the importance of preserving the confidentiality of patients' medical records and related information, such as photographs.

232. Hankins failed to use the reasonable care, skill, or knowledge used by similarly trained cosmetic surgery providers in taking and storing photographs of Plaintiffs. For example, some of these

photographs depict *both* Plaintiffs' face and breasts in a single image. *See* Affidavit of Dr. Nirav Patel, ¶ 6, attached as **Exhibit "2"**. There is no medical reason to include a breast-augmentation Plaintiffs' faces in pre- and post-clinical photographs of the Plaintiffs' breasts. (*See id.*). Indeed, the lack of any medical reason for including Plaintiffs' faces is evidenced by the fact that Hankins did not include Plaintiffs' faces in certain sets of photographs but inexplicably did so in others. A similarly trained cosmetic surgery provider would not include a patient's face when photographing a patient, like Plaintiffs.

233. Hankins further failed to use the reasonable care, skill, or knowledge used by similarly trained cosmetic surgery providers in failing to obtain Plaintiffs' informed, written consent to the taking and storing of photographs. Similarly trained and experienced plastic surgery providers using reasonable care, skill, or knowledge would not take and store photographs of a patient without the patient's informed, written consent. *See* Affidavit of Dr. Nirav Patel Ex. 2, ¶ 7. Hankin's conduct in taking such photographs resulted in the public disclosure of incredibly sensitive and damaging photographs, which were not medically necessary and obtained without notice or consent.

234. Hankins failed to use the reasonable care, skill, or knowledge used by similarly trained cosmetic surgery providers in collecting, storing and maintaining Plaintiffs sensitive PHI and PII. Similarly trained and experience plastic surgery providers using reasonable care, skill, or knowledge would implement greater protective measures to ensure their patients' highly sensitive PHI and PII was not readily exposed to potential Data Breach and threat actors.

235. As a direct and proximate result of Hankin's aforementioned acts, Plaintiffs have suffered—and continue to suffer—the extreme emotional distress alleged above, in an amount subject to proof at trial. Similarly, as a result of Hankin's actions, Plaintiffs now face the cost of necessary constant web-scrubbing consulting services and physical security. These damages are continuing in nature and will be suffered in the future.

236. As a direct and proximate result of Hankins' failure to protect PHI, Plaintiffs and Class Members suffered the various types of damages alleged herein.

237. Plaintiffs and Class Members are entitled to all forms of monetary compensation and injunctive relief set forth herein.

/ / /

DEMAND FOR JURY TRIAL

Please take notice that Plaintiffs demand a trial by jury as to all issues so triable in this action.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all other similarly situated, pray for relief as follows:

1. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as representatives of the Class and Plaintiffs' attorneys as Class Counsel to represent the Class;

2. For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

3. For compensatory damages on behalf of Plaintiffs and the Class;

4. For punitive damages on behalf of Plaintiffs and the Class;

5. For an order of restitution and all other forms of equitable monetary relief;

6. Declaratory and injunctive relief as described herein;

7. For disgorgement and/or restitution as the Court deems appropriate, just, and proper;

8. Awarding Plaintiffs reasonable attorneys' fees, costs, and expenses;

9. Awarding pre- and post-judgment interest on any amounts awarded;

10. For reimbursement for all costs and expenses incurred in connection with the prosecution of these claims; and

11. Awarding such other and further relief as may be just and proper.

Dated this 30th day of December 2024.

THE BOURASSA LAW GROUP

/s/ Jennifer A. Fornetti
MARK J. BOURASSA, ESQ. (NBN 7999)
JENNIFER A. FORNETTI, ESQ. (NBN 7644)
VALERIE S. GRAY, ESQ. (NBN 14716)
2350 W. Charleston Blvd., Suite 100
Las Vegas, Nevada 89102

NICHOLAS A. COLELLA (*pro hac vice*)
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222

RAINA BORRELLI (pro hac vice)
STRAUSS BORRELLI PLLC
980 N. Mich. Ave.
Suite 1610
Chicago, Illinois 60611
Telephone: 872-263-1100
Facsimile: 872-263-1109

RAMZY P. LADAH
LADAH LAW FIRM
517 S. Third Street
Las Vegas, NV 89101
Telephone: (702) 252-0055
Facsimile: (702) 248-0055

CLARK SEEGMILLER
JONATHAN B. LEE
RICHARD HARRIS LAW FIRM
801 S. Fourth Street
Las Vegas, NV 89101

Attorneys for Plaintiffs

CERTIFICATE OF SERVICE

Pursuant to FRCP 5(b), I certify that I am an employee of The Bourassa Law Group, and that on this date I caused to be served a true copy of **SECOND AMENDED CONSOLIDATED CLASS ACTION COMPLAINT** on all parties to this action by the method(s) indicated below:

X by using the Court's CM/ECF Electronic Notification System addressed to:

Gary E. Schnitzer, Esq.
L. Renee Green, Esq.
Marta D. Kurshumova, Esq.
KRAVITZ SCHNITZER JOHNSON & WATSON, CTD.
Email: gschnitzer@ksjattorneys.com
rgreen@ksjattorneys.com
mkurshumova@ksjattorneys.com

Attorneys for Defendants

DATED: This 30th day of December 2024.

/s/ Kylie VanderMiller
Employee of The Bourassa Law Group

EXHIBIT “1”

EXHIBIT “1”

---------- Forwarded message ---------
From: **Hankins and Sohn** <info@hankinsplasticsurgery.com>
Date: Tue, Mar 14, 2023 at 12:00 PM
Subject: Important Information
To: <jentausinga@gmail.com>

Good afternoon,

Hankins & Sohn Plastic Surgery Associates is writing to inform you of a recent data security event that may impact some of your information. We are providing you with information about the event, our response, and steps you can take to better protect your information against the possibility of misuse of your information, should you feel it appropriate to do so.

We recently became aware of allegations by an unknown actor that data was stolen from our network. We are working diligently to assess these allegations and to confirm the nature and scope of the activity. We are also actively working with law enforcement to investigate the activity. We are reviewing the information that we store on our systems to identify current and former patients whose information may have been impacted by this event.

We are unable to confirm which specific patients' information may be at risk; we ultimately made the decision to notify all current or former patients and consults in an abundance of caution. Therefore, we are writing to you given that your information was present on our systems at the time of the incident and was therefore potentially impacted by this event.

While the information may vary by individual, the types of information that could be impacted include name, contact information, date of birth, Social Security number, driver's license information, medical history, consultation notes, and photos.

The unknown actor has threatened to reach out to our patients individually, and we want to provide you with the below steps you can take to protect your personal information, should you feel it appropriate to do so.

Lock Down Your Social Media Profiles

Review your profile settings in your social media accounts to strengthen the privacy of your accounts. Make your account private and limit what can be posted by others on your profile. Enable the option to review tags before they appear on your profile. Only accept friend requests and follows from people that you know. Enable multi-factor authentication to prevent unauthorized logins.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus: Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;

3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

We take this event and the security of information in our care very seriously. Upon learning of this event, we immediately took steps to contact law enforcement and to review the potentially impacted information. We are also taking steps to review our policies and procedures and to implement additional technological safeguards to further secure the information on our systems.
If you have further questions, please call our toll-free dedicated call center at 800-910-5156 Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Please reference the following engagement number: **B087488**.

Our mailing address is:
Hankins Plastic Surgery Associates
60 north pecos road
#100
Henderson, NV 89074

EXHIBIT “2”

EXHIBIT “2”

AFFIDAVIT OF DR. NIRAV PATEL

STATE OF GEORGIA }
} *s.s.*
COUNTY OF COBB }

I, NIRAV B. PATEL, MD, MS, JD, FACS, FCLM being first duly sworn, deposes and says:

1. I am a Board-Certified Plastic and Reconstructive Surgeon. I have been in active independent practice since 2019 and since 2021, I have owned and operated an independent solo plastic surgery practice, Patel Plastic Surgery, located in Marietta, Georgia. I perform all aspects of aesthetic and reconstructive plastic and oculoplastic surgery, with a particular focus on breast aesthetic and reconstructive surgery, Mohs reconstruction, implant-based breast reconstruction, and facial trauma reconstruction. Further information concerning my education, training, and background, experience, practice, and credentials is contained in my *curriculum vitae* attached hereto.
2. My area of practice is substantially similar to the area of practice engaged in by Hankins Plastic Surgery, Dr. W. Tracy Hankins and Dr. Samuel M. Sohn, at the time of the alleged professional negligence. Like myself, both Dr. W. Tracy Hankins and Dr. Samuel M. Sohn are certified by the American Board of Plastic Surgery and Active Members of the American Society of Plastic Surgeons.
3. I have reviewed the following materials, records, and information concerning Plaintiffs Jennifer Tausinga, Alysia Wrenn, Olga Romashova, Caroline Aurora, and Sarah Jefferson: pre- and post-operative clinical photographs taken during Plaintiffs' appointments at Defendants' offices; messages and emails sent to the Plaintiffs by computer hackers, who published the website, https://hankinsandsohn.su/; and the allegations in the Complaint.
4. It is my medical opinion, to a reasonable degree of medical certainty, that Hankins Plastic Surgery, Dr. W. Tracy Hankins, and Dr. Samuel M. Sohn, in rendering services to Plaintiffs, failed to use the reasonable care, skill, or knowledge used under similar circumstances by similarly trained and experienced plastic surgery providers.
5. As described in detail in the Complaint, Plaintiffs underwent treatment for aesthetic plastic surgical procedures by the Defendants at their plastic surgery practice in Henderson, Nevada. Jennifer

Tausinga underwent bilateral breast implant removal with bilateral total capsulectomy and bilateral mastopexy (breast lift) by Dr. Sohn on March 10, 2022, with a subsequent in-office bilateral breast and areola scar revision on February 23, 2023. Alysia Wrenn underwent labiaplasty (clitoral hood reduction) on October 1, 2021, with subsequent in-office Kenalog (steroid) injection on October 3, 2022. Defendants also evaluated Ms. Wrenn in consultation for breast procedures including areolar reduction and autologous fat grafting to the labia and breasts. Olga Romashova underwent bilateral breast augmentation on December 30, 2015 by Dr. Hankins and subsequently underwent injection of dermal filler by Defendants' staff on June 27, 2016 and on December 16, 2016. Caroline Aurora underwent removal of saline breast implants and replacement with silicone breast implants, combined with mastopexy by Dr. Hankins on February 23, 2022. Defendants obtained preoperative photographs of Sarah Jeffersons' face, breasts, and abdomen.

6. Defendants Hankins Plastic Surgery, Dr. W. Tracy Hankins, and Dr. Samuel M. Sohn failed to use reasonable care, skill, or knowledge in taking and storing sensitive clinical photographs of the Plaintiffs. Defendants obtained photographs of Ms. Tausinga's breasts. Defendants obtained photographs of Ms. Wrenn's external genitalia. Defendants obtained photographs of Ms. Romashova's and Ms. Aurora's faces and breasts. Defendants obtained photographs of Ms. Jefferson's face, breasts, abdomen, and buttocks. Plastic surgeons routinely handle patient photography and should use reasonable care, skill, or knowledge in safeguarding patient photographs. For a patient solely seeking a breast-related procedure, there is no medical reason to include that patient's face in pre- and post-clinical photographs of the patient's breasts. This is supported by Defendants' own inexplicable decision to include Plaintiffs' faces in certain sets of photographs, yet not in others. It is my professional opinion, to a reasonable degree of medical certainty, that a similarly trained and experienced plastic surgeon using reasonable care, skill, or knowledge would not take and store photographs of a breast augmentation, breast lift (mastopexy), or breast reduction patient's breasts that included the patient's face. My opinion is supported by the American Society of Plastic Surgeons' "Photographic Guidelines in Plastic Surgery" (attached hereto), which provides that when taking photographs of a patient's breasts, the photographer should position the patient's clavicles at the top of the frame, excluding the patient's face. Both

Dr. W. Tracy Hankins and Dr. Samuel M. Sohn are Active Members of the American Society of Plastic Surgeons.

7. Defendants Hankins Plastic Surgery, Dr. W. Tracy Hankins, and Dr. Samuel M. Sohn failed to use reasonable care, skill, or knowledge in failing to obtain Plaintiffs' informed, written consent to the taking and storing of photographs. It is my professional opinion, to a reasonable degree of medical certainty, that a similarly trained and experienced plastic surgeon using reasonable care, skill, or knowledge would not take and store photographs of a patient without the patient's informed, written consent to the taking and storage of such photographs.
8. It is my expert opinion that Defendants' breaches of the standard of care in plastic surgery caused the harms and losses sustained by the Plaintiffs.
9. I specifically reserve the right to add to, amend, or subtract from this Affidavit as new evidence comes into discovery or as new opinions are formulated.

I DECLARE UNDER PENALTY OF PERJURY UNDER THE LAW OF THE STATE OF NEVADA THAT THE FOREGOING IS TRUE AND CORRECT

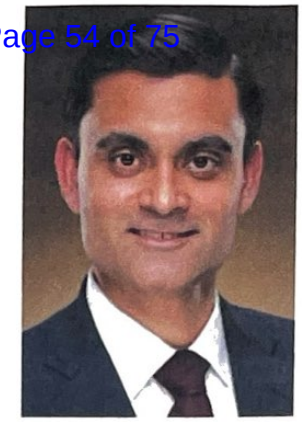
Respectfully submitted,

By: _____
Dr. NIRAV PATEL

SUBSCRIBED AND SWORN to before me on this
6th day of September, 2024

_____
Notary Public

AVERY USHER NOTARY PUBLIC EXPIRES GEORGIA November 23, 2025 CHATHAM COUNTY



Nirav B. Patel, MD, MS, JD, FACS, FCLM
1519 Johnson Ferry Road, Suite 250
East Cobb (Marietta), GA 30062
Office: (470) 395-6932
Fax: (470) 395-6951
Email: nirav.patel@drpatelplasticsurgery.com
LinkedIn: https://www.linkedin.com/in/drpatelplasticsurgery/

EDUCATION

University of Rochester, School of Medicine & Dentistry, Rochester, NY Doctor of Medicine	08/07 – 05/11
New York University, Graduate School of Arts & Science, New York, NY Master of Science in Biology	06/02 – 01/05
Brooklyn Law School, Brooklyn, NY Juris Doctor	06/00 – 06/03
Princeton University, Princeton, NJ Artium Baccalaureus in Economics	09/96 – 05/00

CLINICAL EXPERIENCE & TRAINING

Patel Plastic Surgery, East Cobb (Marietta), GA *Owner – Plastic, Reconstructive, Aesthetic, & Oculoplastic Surgery*	01/21 – present
Wellstar North Fulton Hospital, Roswell, GA *On Call Plastic Surgeon (includes Maxillofacial Trauma)* *Adjunct Clinical Faculty, General Surgery Residency Program*	09/21 – present 03/23 – present
Wellstar Kennestone Hospital, Marietta, GA *Maxillofacial Trauma Surgeon*	03/23 – 06/23 05/19 – 12/20
Comprehensive Medical Services, LLC, Atlanta Metropolitan Area, GA *Contract Employee – Wound Care Management*	06/21 – 03/22
Aesthetic Physicians, PC, Atlanta, GA *Plastic Surgeon – Laser Liposuction*	01/21 – 06/21
Marietta Plastic Surgery, Marietta, GA *Associate Plastic Surgeon*	01/19 – 12/20
Mark Codner, MD Plastic Surgery, Atlanta, GA *Oculoplastic & Aesthetic Surgery Fellowship*	07/18 – 12/18

August 27, 2024:
This document is not a retention agreement. A retention agreement is always required in order to be retained.

Grotting Plastic Surgery, Birmingham, AL
*Breast & Aesthetic Surgery Fellowship (Endorsed by **The Aesthetic Society**)* 07/17 – 06/18
*Instructor/Fellow, **University of Alabama at Birmingham Department of Surgery*** 07/17 – 06 18

University of California, Davis Medical Center, Sacramento, CA
*Visiting Professor, **Division of Plastic & Reconstructive Surgery*** 12/22
*Administrative Chief Resident, **Division of Plastic & Reconstructive Surgery*** 07/16 – 06/17
*Member, **Program Evaluation Committee** (Independent Program Format)* 07/16 – 06/17
*Senior Resident, **Division of Plastic & Reconstructive Surgery*** 07/14 – 06/16
*Junior Resident (including Internship), **Department of General Surgery*** 06/11 – 06/14

ACTIVE HOSPITAL AFFILIATIONS

Wellstar North Fulton Hospital, Roswell, GA	*(Active)*	12/20 – present
	(Teaching)	03/23 – present
Northside Hospital Atlanta, Atlanta, GA	(*Courtesy*)	01/23 – present
(includes **Northside Alpharetta Surgery Center**)		01/23 – present
Northside Cherokee Hospital, Canton, GA	*(Courtesy)*	12/22 – present
		02/19 – 12/20
Northside Hospital Forsyth, Cumming, GA	*(Courtesy)*	01/21 – present

BIOMEDICAL RESEARCH EXPERIENCE

University of Rochester Medical Center, Rochester, NY
*Clinical Research Assistant, **Division of Plastic & Reconstructive Surgery*** 08/08 – 08/10
*Clinical Research Assistant, **Department of Emergency Medicine*** 06/08 – 04/09

North Shore-Long Island Jewish Health System (Feinstein Institute), Manhasset, NY
*Research Assistant Technician, **Kevin Tracey Lab*** 08/05 – 06/07

LICENSES & CERTIFICATIONS

American Board of Plastic Surgery
Diplomate (Board Certified) 11/20 – 12/30

American College of Surgeons
Fellow 10/21 – present

American College of Legal Medicine
Fellow (Licensed Attorney & Licensed Physician) 08/18 – present

Georgia Composite Medical Board
Georgia Medical License, *#079981* 03/18 – 02/26

Drug Enforcement Administration
DEA Registration, *#FP3435078* 08/12 – 03/27
DEA Registration, *#FP9928663 [for Aesthetic Physicians, PC only]* 01/21 – 03/24

NYS Supreme Court, Appellate Division, 2nd Department, 10th Judicial District
Member, New York Bar, Attorney Registration *#4202222* 05/04 – 02/26

Medical Board of California
California Medical License, *#A122094* 07/12 – 02/24

California Board of Registered Nursing (John E. Hoopman, CMLSO)
Laser Safety / Biophysics of Laser Applications, *Provider #15405* 08/14

Alabama Medical Licensure Commission
Alabama Medical License, *#MD.35753* 02/17 – 12/18
Alabama Controlled Substances Registration, *#ACSC.35753* 02/17 – 12/18

Advanced Cardiovascular Life Support (including Basic Life Support)
Recertification, Marietta, GA (online) 11/23
Recertification, Marietta, GA (online) 01/22
Recertification, Marietta, GA (at Marietta Plastic Surgery) 02/20
Recertification, Birmingham, AL (online) 03/18
Recertification, Rancho Cordova, CA 07/15
Recertification, Roseville, CA 04/13
Initial Certification, Rochester, NY 05/11

POSTGRADUATE COURSES, MEETINGS, & CONTINUING MEDICAL/LEGAL EDUCATION

Plastic Surgery The Meeting 2024, San Diego, CA ***[Faculty]*** 09/24 *(expected)*

33rd Annual King & Spalding Health Law & Policy Forum, Atlanta, GA 03/24

Medical Malpractice Survival Training for Physicians / SEAK, Inc.
Nadine Nasser Donovan, Esq. 11/23

Plastic Surgery The Meeting 2023, Austin, TX ***[Faculty]*** 10/23

DEA Medication Access and Training Expansion (MATE) Act Compliance 08/23

30th Anniversary National Expert Witness Conference, Clearwater Beach, FL 05/23

Plastic Surgery The Meeting 2022, Boston, MA ***[Faculty]*** 10/22

Plastic Surgery The Meeting 2022, Senior Residents Conference *[Faculty]* 10/22

Georgia Society of the ACS Annual Meeting, St. Simons Island, GA 08/22

GSPS Annual Meeting, Lake Lanier Island, GA 07/22

SESPRS Annual Meeting, Orlando, FL 06/22

37th Annual Atlanta Breast Surgery Symposium / SESPRS 01/22

2nd SESPRS / ISAPS Periorbital & Facial Symposium, Atlanta, GA 01/22

Allergan Medical Institute – Surgical Solutions Symposium 11/21
(including Smooth Tissue Expander Bioskills Cadaver Lab – Assisted with Video Demonstration)

Plastic Surgery The Meeting 2021, Senior Residents Conference *[Faculty]* 10/21

American College of Surgeons Clinical Congress
Regional Anesthesia Techniques: Abdominal Wall and Pectoral Blocks 10/21
Fundamentals of Oncoplastic Breast Surgery 10/21

Wound Care Certification Course
WoundEducators.com® 08/21

SESPRS Annual Meeting, Hilton Head Island, SC 06/21

How to Be an Effective Expert Witness / SEAK, Inc.
James J. Mangraviti, Jr., Esq. & Kelly J. Wilbur, Esq. 06/21

ASPS Practice Innovations 03/21

How to Start, Build, and Run a Successful Expert Witness Practice / SEAK, Inc.
James J. Mangraviti, Jr., Esq. 12/20

ABMS Member (ABPS) Board Certification: issued via the AMA 12/20

ASAPS Residents' Symposium: The Business of Launching Your Practice, New York, NY
Nolan Karp, MD & Ashley Gordon, MD 12/20

2020 Life-Long Learning Exercise (L3E): Aesthetic In-Service / ASPS 07/20

2020 In-Service Exam / American Society of Plastic Surgeons 04/20

36th Annual Atlanta Breast Surgery Symposium / SESPRS 01/20

1st SESPRS / ISAPS Periorbital & Facial Symposium, Atlanta, GA 01/20

Musculoskeletal Transplant Foundation Technical Education, Edison, NJ 12/19

2019 ASPS Oral Board Preparation Course / ASPS, Rosemont, IL 08/19

ASPS University: Essentials of Medical Coding (Bundle) 08/19

2019 Life Long Learning Experience / American Society of Plastic Surgeons 05/19

2019 In-Service Exam / American Society of Plastic Surgeons 03/19

35th Annual Breast Surgery Symposium / SESPRS, Atlanta, GA 01/19

ASAPS Residents' Symposium: The Business of Launching Your Practice, New York, NY
Gary Tuma, MD & Nolan Karp, MD 12/18

Mentor Innovation Training, Dallas, TX (2nd attendance) 10/18

Sciton Live Demonstration & Hands On Workshop: Halo Hybrid Laser 10/18

Plastic Surgery The Meeting 2018, Chicago, IL 09/18

Sciton Advanced Aesthetic & Laser Symposium, Atlanta, GA 09/18

Allergan Medical Institute Illumination Tour & Training, Atlanta, GA 09/18

Galderma Aesthetic Injector Network, Peer-to-Peer Training, Atlanta, GA 07/18

The Aesthetic Meeting 2018, New York, NY 04/18

Thermi Temperature Controlled Radiofrequency Training, Birmingham, AL 12/17

ASPS Written Board Preparation Course, Rosemont, IL 08/17

Operation Smile Resident's Leadership Conference, Manila, Philippines 07/17

CSPS 67th Annual Meeting, San Francisco, CA 05/17

The Aesthetic Meeting 2017, San Diego, CA 04/17

Dallas Cosmetic Surgery & Rhinoplasty Symposia, Dallas, TX 03/17

SESPRS Oculoplastic & Breast Symposia, Atlanta, GA 01/17

Mentor Innovation Training, Dallas, TX (1st attendance) 10/16

ASPS Senior Residents Conference & Residents Day, Los Angeles, CA 09/16

ASAPS Resident Oculoplastic Surgery Course, Santa Monica, CA
Glenn Jelks, MD & Elizabeth Jelks, MD 05/16

ASAPS Residents' Symposium: The Business of Launching Your Practice, Dallas, TX
Mark Codner, MD & Salvatore Pacella, MD, MBA 12/15

ASPS Senior Residents Conference & Residents Day, Boston, MA 10/15

Galderma Aesthetic Dermatology Training Session, Sacramento, CA 07/15

Two Stage Implant Breast Reconstruction, Monterey, CA
Peter Cordeiro, MD 05/15

ASAPS Resident Laser Training Course, Monterey, CA
Jeffrey Kenkel, MD, John Hoopman, & Robert Aycock, MD 05/15

Plastic Surgery Foundation – Research Fundamentals Course, Seattle, WA 05/15

UC Davis Department of Surgery Abdominal Reconstruction Cadaver Lab Program
Sacramento County Coroner's Office, Sacramento, CA 01/15

AO Craniomaxillofacial Trauma Principles Course, St. Louis, MO 08/14

Sciton Laser Physics, Safety, and Tissue Interactions Course, Larkspur, CA 08/14

Advanced Trauma Life Support, Sacramento, CA 11/12

PEER-REVIEWED PUBLICATIONS

1. Hollier LH Jr, Davis MJ, Abu-Ghname A, Patel NB, Pacitti S Esq, Reece EM. Are You Ready to Negotiate Your First Employment Contract? Experience of More Than 700 Plastic Surgeons. **Plast Reconstr Surg.** 2021 Mar 1;147(3):761-771.

2. Song P, Patel N, Pu LLQ. Reoperation of Lower Extremity Microsurgical Reconstruction When Facing Postsplenectomy Thrombocytosis. **Plast Reconstr Surg Glob Open.** 2019 Nov 12;7(11):e2492. eCollection 2019 Nov.

3. Asserson DB, Patel NB, Arsalai MM, Pu LLQ. The plastic surgeon as employee: Survey of the American Society of Plastic Surgeons. **J Plast Reconstr Aesthet Surg.** 2019 Jan;72(1):137-171. Epub 2018 Nov 13.

4. Grotting JC, Patel NB. Commentary on: Intra-Areolar Pexy: The "Compass Rose" Suture Technique for Small and Moderate Areola Herniation. **Aesthet Surg J**. 2018 Jul 10.

5. Jairam A, Song P, Patel NB, Wong MS. Pressure Sores and Systemic Inflammatory Response Syndrome: UC Davis Quality Improvement Initiative. **Ann Plast Surg**. 2018 May;80(5S Suppl 5):S308-S310. Presented at the Regular Paper Session of the 67th Annual Meeting of the **California Society of Plastic Surgeons**, May 28, 2017, San Francisco, CA. Presented at the 97th Annual Meeting of the **American Association of Plastic Surgeons,** April 10, 2018, Seattle, WA. [Presented by Jairam A.]

6. Patel NB, Coombs DM, Arsalai M, Li C-S, Liu Y, Stevenson TR, Pu LLQ. The Plastic Surgeon as Employee: A Pilot Survey of the California Society of Plastic Surgeons. **Ann Plast Surg**. 2017 May;78(5 Suppl 4):S238-S242. Presented at UC Davis Medical Center Division of Plastic Surgery **Grand Rounds**, February 9, 2016, Sacramento, CA. Presented at UC Davis Medical Center Department of Surgery **Resident Research Symposium**, April 19, 2016, Sacramento, CA. Presented for the **Resident Competition** at the 66th Annual Meeting of the **California Society of Plastic Surgeons**, May 28, 2016, Santa Monica, CA. Earned **2nd Prize** at Inaugural UC Davis Division of Plastic Surgery **Academic Day Resident Research Competition**, June 7, 2016, Sacramento, CA (**adjudicated by Dr. John Persing**, Section Chief, Yale University).

7. Coombs DC, Patel NB, Zeiderman M, Wong MS. The Vertical Rectus Abdominis Musculocutaneous Flap as a Versatile and Viable Option for Perineal Reconstruction. **EPlasty.** 2017 Jan 16;17:ic2. eCollection 2017.

8. Song P, Patel NB, Gunther S, Li C-S, Liu Y, Lee CYG, Kludt NA, Patel KB, Ali MR, Wong MS. Body Image and Quality of Life: Changes With Gastric Bypass and Body Contouring. **Ann Plast Surg.** 2016 May;76: S211-S216. Presented for the **Resident Competition** at the 65th Annual Meeting of the **California Society of Plastic Surgeons**, May 24, 2015, Monterey, CA [by Patel

NB], and at the **American Society of Plastic Surgeons Meeting**, October 17, 2015, Boston, MA [by Song P].

9. Patel NB, Wong MS. Extended fasciocutaneous flaps for autologous augmentation mastopexy with upper body lift after massive weight loss: an early experience. **Ann Plast Surg**. 2015 May;74 Suppl 1:S41-5. Presented at the **Resident Competition** for the 64th Annual Meeting of the **California Society of Plastic Surgeons**, May 25, 2014, Newport Beach, CA.

10. Chavan S, Hudson L, Li J, Ochani M, Harris Y, Patel N, Katz D, Scheinerman J, Pavlov V, Tracey K. Identification of Pigment Epithelium-Derived Factor as an adipocyte-derived inflammatory factor. **Mol Med**. 2012 Oct 24;18:1161-8.

11. Koltz PF, Sbitany H, Myers RP, Shaw RB, Patel N, Girotto JA. Reduction Mammaplasty in the Adolescent Female: The URMC Experience. **Int J Surgery**. 2011;9(3):229-32.

12. Bruchfeld A, Goldstein RS, Chavan S, Patel NB, Rosas-Ballina M, Kohn N, Qureshi AR, Tracey KJ. Whole blood cytokine attenuation by cholinergic agonists ex vivo and relationship to vagus nerve activity in rheumatoid arthritis. **J Intern Med**. 2010 Jul;268(1):94-101.

13. Rosas-Ballina M, Goldstein RS, Gallowitsch-Puerta M, Yang L, Valdés-Ferrer SI, Patel NB, Chavan S, Al-Abed Y, Yang H, Tracey KJ. The selective alpha7 agonist GTS-21 attenuates cytokine production in human whole blood and human monocytes activated by ligands for TLR2, TLR3, TLR4, TLR9, and RAGE. **Mol Med**. 2009 Jul-Aug;15(7-8):195-202.

14. Parrish WR, Rosas-Ballina M, Gallowitsch-Puerta M, Ochani M, Ochani K, Yang LH, Hudson L, Lin X, Patel N, Johnson SM, Chavan S, Goldstein RS, Czura CJ, Miller EJ, Al-Abed Y, Tracey KJ, Pavlov VA. Modulation of TNF release by choline requires alpha7 subunit nicotinic acetylcholine receptor-mediated signaling. **Mol Med**. 2008 Sep-Oct;14(9-10):567-74.

15. Goldstein RS, Bruchfeld A, Yang L, Qureshi AR, Gallowitsch-Puerta M, Patel NB, Huston BJ, Chavan S, Rosas-Ballina M, Gregersen PK, Czura CJ, Sloan RP, Sama AE, Tracey KJ. Cholinergic anti-inflammatory pathway activity and High Mobility Group Box-1 (HMGB1) serum levels in patients with rheumatoid arthritis. **Mol Med**. 2007 Mar-Apr;13(3-4):210-5.

16. Goldstein RS, Bruchfeld AN, Gallowitsch-Puerta M, Patel N, Yang H, Rosas-Ballina M, Lee DC, Czura CJ, Sama AE, Tracey KJ. Vagus Nerve Activity and Cytokine Responsiveness in Patients with Rheumatoid Arthritis. **Journal of Investigative Medicine**. 2006;54(2_suppl):377-377.

PUBLISHED ABSTRACTS

1. Patel NB, Arsalai M, Stevenson TR, Parent EW, Pu LLQ. The Plastic Surgeon as Employee. **Plast Reconstr Surg Glob Open.** 2016 Sept; 4(9 Suppl): 36-37. Abstract presented as **Podium Presentations** at the **Practice Management** and **Residents Day** Sessions of the **American Society of Plastic Surgeons Meeting**, September 2016, Los Angeles, CA.

2. Patel NB, Gunther S, Song P, Li C-S, Kludt NA, Lee CYG, Hearney SM, Patel KB, Ali MR, Wong MS. Abstract 46: Body Image And Quality Of Life: Changes With Gastric Bypass Surgery And Body Contouring. **Plast Reconstr Surg.** 135(5S):40, May 2015. Presented at the 60th Annual Meeting of the **Plastic Surgery Research Council**, May 15, 2015, Seattle, WA.

3. Sbitany H, Koltz PF, Patel N, Girotto JA, Vega SJ, Langstein HN. Quadriceps Muscle Function Following Harvest of the Rectus Femoris Muscle as a Myofascial Flap for Complex Groin Wound Reconstruction. **American Association of Plastic Surgeons**, 2009 Annual Meeting. [Presented by Koltz PF.]

4. Cushman JT, Patel NB, Jones CM, Swor RA, E. Lerner EB, Shah MN. A Comparison of the Ohio and American College of Surgeons Guidelines in Identifying Trauma Center Need for Older Adults. **National Association of EMS Physicians**, 2009 Annual Meeting. [Presented by Cushman JT.]

5. Goldstein RS, Bruchfeld A, Gallowitsch-Puerta M, Patel NB, Huston B, Rosas-Ballina M, Czura CJ, Tracey KJ. Cholinergic Agonists Inhibit LPS Induced Whole Blood TNF Release Ex Vivo in Patients with Severe Sepsis: A Pilot Study. Acad Emerg Med. 2007 May;14(5 Suppl 1):S185-6. **Society for Academic Emergency Medicine**, 2007 Annual Meeting. [Presented by Goldstein RS.]

PRESENTATIONS

1. Patel NB, Byrd M, Reyero JD, Polis MG, Dennis C. Staying Out of Trouble. **Plastic Surgery The Meeting,** Practice Management Track, September 28, 2024, San Diego, CA. *(forthcoming)*

2. Kavali C, Byrd M, Patel NB, Reyero J. Know Your Worth: Employment Contracts and Rate Negotiations. **Plastic Surgery The Meeting,** Practice Management Track, September 26, 2024, San Diego, CA. *(forthcoming)*

3. Patel NB, Miller JW, Mackenzie DD, Arsalai M, Claxton A, Dennis C. Key Legal Issues for Plastic Surgeons. **Plastic Surgery The Meeting,** Practice Management Track, October 29, 2023, Austin, TX.

4. Patel NB, Adatto BE, Bird DW, Wong MS. Plastic Surgeons as Employees: Best Practices and Lessons Learned. **Plastic Surgery The Meeting,** Practice Management Track, October 27, 2023, Austin, TX.

5. Patel NB. CEO Forum. **Georgia Association of Physicians of Indian Heritage,** June 17, 2023, Atlanta, GA.

6. Patel NB, Ravichandar H. Medfinity: The Future of Technology and Medicine. **The Gwinnett School of Mathematics, Science and Technology,** February 15, 2023, Lawrenceville, GA.

7. Patel NB. What Can You Ask for in a Contract? **UC Davis Medical Center Division of Plastic Surgery Grand Rounds,** December 13, 2022, Sacramento, CA.

8. Patel NB, Wong MS, Reyero JD, Basu CB. Plastic Surgeons as Employees: Best Practices and Lessons Learned. **Plastic Surgery The Meeting,** Practice Management Track, October 30, 2022, Boston, MA.

9. Francis SH, Meyers PL, Patel NB, Suber JS, Stranix JT. Q&A Panel: Practice Type. **Plastic Surgery The Meeting,** Senior Residents Conference, October 27, 2022, Boston, MA.

10. Patel NB. What Can You Ask for in a Contract? **Plastic Surgery The Meeting,** Senior Residents Conference, October 27, 2022, Boston, MA.

11. Patel NB, Byrd MS, Adatto BE, Reece EM. First Contract: Navigating the Waters. **American Society of Plastic Surgeons,** October 22, 2022, Marietta, GA; Dallas TX; Scottsdale, AZ. [Virtual Live Recording on Zoom, August 24, 2022.]

12. Patel NB. What Can You Ask for in a Contract? **University of Rochester Division of Plastic Surgery Grand Rounds,** July 14, 2022, Rochester, NY. [Virtual Meeting on Zoom.]

13. Patel NB. What Can You Ask for in a Contract? **Plastic Surgery The Meeting,** Senior Residents Conference, October 28, 2021, Atlanta, GA.

14. Patel NB. Fellowship Panel – Aesthetic Surgery. **University of Washington Plastic Surgery Residency Program,** September 15, 2021, Seattle, WA. [Virtual Meeting on Zoom.]

15. Codner MA, Patel NB, Krochonis J, McConville R, Patterson E. Facial and Periorbital Rejuvenation with Non-surgical Techniques. **North Carolina Society / South Carolina Society of Plastic Surgeons,** Joint Annual Meeting, November 3, 2018, Kiawah Island, SC. [Presented by Codner MA.]

16. Patel NB, Wu C, Grotting JC. Saline Implant Deflation in Revisional Aesthetic Breast Surgery. **American Society for Aesthetic Plastic Surgery,** Endorsed Fellowship Forum & Practice Changers, April 28-29, 2018, New York, NY.

17. Grotting JC, Patel NB. Plastic Surgery 'Triumph': Otoplasty. **American Alpine Workshop in Plastic Surgery,** February 12-16, 2018, Telluride, CO. [Presented by Grotting JC.]

18. Grotting JC, Patel NB. The 'Turderous' Breast. **American Alpine Workshop in Plastic Surgery,** February 12-16, 2018, Telluride, CO. [Presented by Grotting JC.]

19. Grotting JC, Patel NB. I've Been Hacked! Cybersecurity for the Plastic Surgeon. **Florida Society of Plastic Surgeons,** December 17, 2017, The Breakers, Palm Beach, FL. [Presented by Grotting JC.]

20. Grotting JC, Rhee S, Patel NB. Upper Blepharoplasty Based on Individual and Ethnic Variations of Anatomy. **The Aston Baker Cutting Edge 37th Aesthetic Surgery Symposium,** November 30, 2017, New York, NY. [Presented by Grotting JC.]

21. Grotting JC, Patel NB. Fat Grafting The Face – What I Have Learned. 2017 "Siglo XXI," 22° **Simposio Internacional de Cirugía Plástica,** September 21, 2017, Buenos Aires, Argentina. [Presented by Grotting JC.]

22. Patel NB, Coombs DM, Pu LLQ. Plastic Surgeon Wannabes: Dangers of Non-Core Aesthetic Providers. Presented at **UC Davis Medical Center Division of Plastic Surgery Grand Rounds**, March 28, 2017, Sacramento, CA. Presented at the Clinical Pearls Session of the 67th Annual Meeting of the **California Society of Plastic Surgeons**, May 28, 2017, San Francisco, CA.

23. Patel NB. Operation Smile: Lessons Learned in Yunnan, China. Presented at **UC Davis Medical Center Division of Plastic Surgery Grand Rounds**, September 6, 2016, Sacramento, CA.

24. Patel NB. Rhinoplasty. Presented at **UC Davis Medical Center Division of Plastic Surgery Selected Readings Conference**, January 22, 2016, Sacramento, CA.

25. Patel NB, Stevenson TR. Reflections on Plastic Surgery in Port-de-Paix, Haiti. Presented at **UC Davis Medical Center Division of Plastic Surgery Grand Rounds**, September 15, 2015, Sacramento, CA. Featured lecture at the UC Davis School of Medicine **Dean's Global Health Night**, June 2, 2015, Sacramento, CA.

26. Patel NB. Facelifts and Alternatives. Presented at **UC Davis Medical Center Division of Plastic Surgery Grand Rounds**, September 16, 2014, Sacramento, CA.

ARTICLES & BOOK CHAPTERS

1. Patel NB, Reyero J. Perspectives on Plastic Surgery Non-Competes. **American Society of Plastic Surgeons: Plastic Surgery News.** April/May 2023.

2. Grotting JC, Patel NB, Vinyard WJ. Reoperative Rhytidectomy. **The Art of Aesthetic Surgery: Principles and Techniques.** 3rd ed. New York: Thieme; 2020.

3. Basu CB, Patel NB. Internal Bra Technique in the Breast with Poor Soft Tissue Support. **Cosmetic Breast Surgery.** 1st ed. New York: Thieme; 2020.

4. Patel NB, Pu LLQ. Correction of Gynecomastia. **Atlas of Contemporary Aesthetic Breast Surgery.** 1st ed. London: Elsevier; 2020.

MEDIA APPEARANCES & INTERVIEWS

1. Turbulence Ahead? **Plastic Surgery News,** September 2024 Cover Story [interviewed by PSN Managing Editor, Paul Snyder].

2. Checking Out Georgia Philharmonic. **Neighborhood TV Atlanta,** March 27, 2024 [videotaped with reporter Reneé Rayles].

3. GSO Spotlight: Nirav B. Patel, MD. **Georgia Symphony Orchestra,** September 12, 2023 [audiotaped with GSO Executive Director, Suzanne Tucker].

4. Careers in Surgery. **Fulton County Schools (FCS) Innovation Academy,** August 28, 2023 [videotaped with student Cade McNair].

5. Enhance Your Practice Podcast: Medical Malpractice. **American Society of Plastic Surgeons,** July 1, 2023 [audiotaped with ASPS Practice Management Committee Chair, Diana-Yoon Schwartz, MD, PhD].

6. Enhance Your Practice Podcast: Expert Witnessing. **American Society of Plastic Surgeons,** May 15, 2023 [audiotaped with ASPS Practice Management Committee Chair, Diana-Yoon Schwartz, MD, PhD].

7. Enhance Your Practice Podcast: Employment Contracts. **American Society of Plastic Surgeons,** May 15, 2023 [audiotaped with ASPS Practice Management Committee Chair, Diana Yoon-Schwartz, MD, PhD].

8. The price of pretty: Butt injections gone wrong. **Atlanta News First (CBS Affiliate),** April 12, 2023 [videotaped with investigative journalist Ciara Cummings].

VOLUNTEER & OTHER PROFESSIONAL EXPERIENCES

Georgia Philharmonic, Roswell, GA
Principal Cellist (audition won by competitive, double blinded process) 09/23 – present
Dragon Con at *Hyatt Regency Atlanta* 08/24 *(expected)*
Samuel Fordis Young Artists Concerto Competition
Performance at ***Atlanta Symphony Hall (Woodruff Arts Center)*** 02/24
Adjudicator, 1st Round 11/23 – present
Collaboration with ***Georgia State University Orchestra (Rialto Center)*** 11/23
Collaboration with ***Georgia State University Orchestra (Kopleff Recital Hall)*** 10/23
Substitute Cellist, ***Dragon Con*** *(Atlanta, GA)* 08/23 – 09/23

Georgia Symphony Orchestra, Marietta, GA
Assistant Principal Cellist 08/18 – present
Member, Board of Directors 08/19 – 06/20
Handel's Messiah at ***Alpharetta Presbyterian Church*** 12/23
Warriors Alliance Gala at the ***Coca-Cola Roxy*** 05/23
Roy Orbison Hologram Tour Performance at the ***Fox Theatre*** 11/18
Fundraiser Performance at the ***Cherokee Town Club*** 10/18

Atlanta Musicians' Orchestra, Atlanta, GA, Morrow, GA, & Decatur, GA
Soloist – Beethoven Triple Concerto at ***Spivey Hall*** 06/25 *(expected)*
Soloist – Richman "Un Pasto": Concerto for Violin, Cello, & Orchestra
World Première at ***Spivey Hall*** 06/22
Soloist – Fauré Élégie; Elgar Cello Concerto, 4th mvmt 08/19
Principal Cellist 07/18 – 08/23

Atlanta Philharmonic Orchestra, Decatur, GA
Substitute Cellist, "Wings of Hope" Concert at ***First Baptist Church Decatur*** 03/24

Georgia Chamber Music Retreat, Berry College, GA
Winner – 22nd Annual Chamber Music Sight-Reading Competition 07/24

Princeton Alumni Schools Committee (ASC)
Chair, GA—111—Atlanta Region 08/22 – present
Princeternship Host (In-Person Internship for Princeton Students) 01/24
Board Member, Princeton Club of Georgia 08/22 – present
Alumni Interviewer
Greater Atlanta 08/18 – present
Greater Alabama 08/17 – 06/18
Northern California, East Sacramento 08/16 – 06/17
Greater NYC Region, Nassau County 08/06 – 06/07

University of Rochester Alumni: Meliora Collective Mentorship Program
Mentor for Premedical and Medical Students 02/22 – present

Walton Raider Orchestra Guild, Inc. (WROG)
WROG Board Co-President (with spouse Erica Patel) 04/24 – present

The Westminster Schools
JanTerm Educational Partner 01/24 – present

Fulton County School District
Mentor for High School Internship Program 08/22 – 12/22

Gwinnett School of Mathematics, Science, and Technology (GSMST)
Mentor for Junior Fellowship Experience (JFE) 04/21 – 08/22

KPMG Women's PGA Championship, Johns Creek, GA
Volunteer, Medical Staff Services, ***Atlanta Athletic Club*** 06/21

Samford Orchestra, Birmingham, AL
Section Cellist 08/17 – 04/18

University of Alabama at Birmingham Concert Choir
Principal Cellist 02/18 – 03/18

Red Mountain Chamber Orchestra, Birmingham, AL 01/18 – 02/18
Principal Cellist

Camellia Symphony Orchestra, Sacramento, CA
Alternate Principal & 3rd Chair Cellist 08/14 – 04/17
Street Medicine Sacramento Fundraiser Performance ***(Run to Feed the Hungry)*** 11/16
Fundraiser Duo Performances at ***The Sutter Club*** 08/15 & 08/16
Collaboration with ***Sacramento Philharmonic & Opera*** 06/15
Nepal Benefit Fundraiser Performance 05/15
Collaboration with ***UC Davis Symphony Orchestra (Mondavi Center)*** 05/15

Operation Smile, Chuxiong City Hospital, Yunnan Province, China 07/16

Centre Médical Béraca, La Pointe des Palmistes, Port-de-Paix, Haiti 03/15
Faculty: Thomas R. Stevenson, MD *(Chief, Ret., UC Davis Division of Plastic Surgery)*

SOCIETY & COMMITTEE MEMBERSHIPS

American Society of Plastic Surgeons
Member, ***Legislative Advocacy Committee*** 09/15 – 09/24
Regulatory Subcommittee Vice Chair 10/23 – 09/24
Participant, ***Advocacy Summit & Regional Fly-Ins,*** Washington, D.C. 12/23
11/15 – 06/19
Member, ***Medical Liability Reform SME Task Force*** 09/15 – 09/17
Co-Chair, ***Practice Management Committee*** 10/22 – 09/24
Peer Reviewer, ***Plastic and Reconstructive Surgery – Global Open*** *[CME]* 05/22 – present
Member, ***Young Plastic Surgeons (YPS) Forum*** 07/21 – present
Member, ***Professional Liability Insurance Committee*** 09/11 – 09/12
Candidate for Membership 10/18 – 07/21

American College of Surgeons	
Fellow	10/21 – present
Member, ***Young Fellows Association (YFA)***	09/21 – present
Liaison, ***ACS Board of Governors Grassroots Workgroup***	02/22 – 10/25
Member, ***Georgia Society of the American College of Surgeons (GSACS)***	01/22 – present
Initiate	06/21 – 10/21
Resident and Associate Society Member	07/11 – 06/17
American Medical Association	
Delegate/Representative, ***Private Practice Physicians Section (PPPS)***	04/21 – present
Member	08/07 – present
The Aesthetic Society ***(formerly the American Society for Aesthetic Plastic Surgery)***	
Member	04/21 – present
Endorsed Aesthetic Surgery Fellow	07/17 – 06/18
Southeastern Society of Plastic and Reconstructive Surgeons	
Member	06/21 – present
Candidate for Membership	01/18 – 06/21
Georgia Society of Plastic Surgeons	
Member	05/22 – present
Medical Association of Georgia	
Member	05/19 – present
Participant, ***MAG House of Delegates,*** Stone Mountain, GA	10/19
Georgia Association of Physicians of Indian Origin	
Lifetime Member	06/23 – present
Greater Cobb County Medical Society	
Member, ***Board of Directors***	02/24 – present
General Member	02/19 – 12/20
California Society of Plastic Surgeons	05/13 – 06/17
Resident Auditor, ***CSPS Council from the North***	07/15 – 06/16
Member, ***2016 CSPS Scientific Program Committee***	07/15 – 06/16
University of California, Davis Surgical Alumni Association	07/17 – present
Greater Sacramento Society of Plastic Surgeons	07/14 – 06/17
Rochester Academy of Medicine, Rochester, NY	
Member, ***Board of Trustees***	08/08 – 05/11

HONORS, AWARDS, & GRANTS

Most Press Mentions 2023 [Top 10% Most Mentioned Clinician in Press]
Most Cited 2022 [Top 10% Most Cited Clinician]
Doximity *[doximity.com]* 05/23 & 12/23

Visiting Professor, *University of California, Davis Division of Plastic Surgery* 12/22

Top Doctor, 2021, 2022, 2023
Find A Top Doc *[findatopdoc.com]* 08/21 – 05/24

Resident Scholarships, *ASPS Advocacy Summits*
American Society of Plastic Surgeons / Allergan / Mentor 03/17 & 04/18

ASAPS Resident Travel Scholarships
Aesthetic Surgery Education and Research Foundation (ASERF) 11/16 & 04/18

Resident/Fellow Inspirational Mentorship Award, *UC Davis Health*
UC Davis School of Medicine, Office of the Vice Chancellor 02/17

House Staff Resident Professionalism Award, *UC Davis Health*
UC Davis School of Medicine Alumni Association 07/16

Second Prize, *UC Davis Plastic Surgery Academic Day – Resident Research Competition*
Visiting Plastic Surgery Section Chief, Dr. John Persing (Yale University) 06/16

Stryker Fellowship, *Operation Smile, Resident Leadership Program* 08/15

Clinical Research Award, *University of Rochester School of Medicine* 06/08

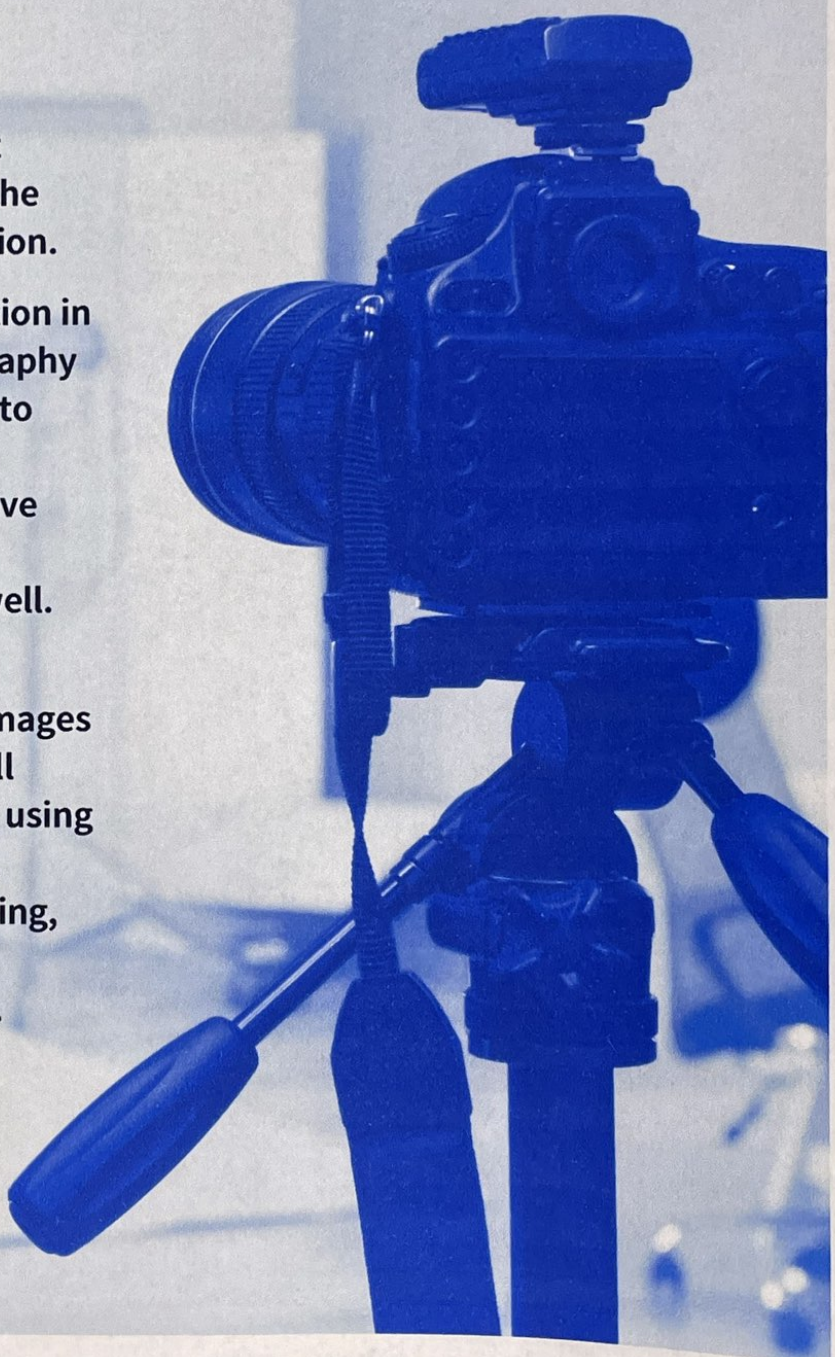
Dean's Merit Scholar, *Brooklyn Law School* 06/00

PHOTOGRAPHIC GUIDELINES IN PLASTIC SURGERY

The standard photographic views illustrated in this brochure were established by the American Society of Plastic Surgeons. These poses best document the pertinent anatomy of the patient without distortion or distraction.

Referencing the images and information in this brochure during patient photography will help any plastic surgery practice to capture consistent pre- and post-op images. When capturing post-operative photos, it is a good idea to have the patient's pre-op images on hand as well.

These guidelines help ensure that comparisons of pre-op and post-op images will yield meaningful observations. All clinical photographs should be taken using the same equipment and procedures. Camera, lighting, magnification, framing, patient positioning and patient preparation all need to be consistent.



AMERICAN SOCIETY OF PLASTIC SURGEONS®

THE PLASTIC SURGERY FOUNDATION™

SING THIS PHOTOGRAPHIC GUIDELINES CHART

CAMERA TO PATIENT DISTANCE

One of the goals of standardized photography is to maintain consistent magnification from photo to photo. For a given camera system, this may be achieved by controlling the distance from camera to patient. However, the distance required for a particular magnification is not the same for all camera systems—it is affected by the size of the imaging sensor and the focal length of the lens.

Each series of images in this chart lists a target area size and a 35mm reproduction ratio. The camera-to-patient distance will need to be filled in for the imaging system being used. This may be accomplished as follows:

1. On a wall or other flat, stationary surface, place tape marks that describe the target area. To calibrate for a 1:10 reproduction ratio, for example, tape a box that is 36cm x 24cm.

2. Make sure the correct lens is mounted to the camera. If a zoom lens is being used, make sure it is set to the proper focal length. (Note: Always use the same focal length for a particular view.)

3. Holding the camera at the same height as the tape marks and looking through the camera's viewfinder, determine the distance from the wall at which the tape marks are in sharp focus and positioned at the edges of the image area.

4. Measure the distance from the camera to the wall and record it in the appropriate location on this chart.

5. If you are using an indexable manual-focus lens, mark the setting on the focus ring.

COLOR CODING

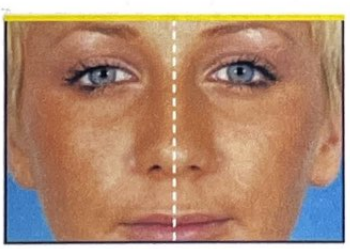
Each target area listed in this chart is marked with a corresponding color. Using these same colors for indexing the camera lens and marking camera-to-patient distances on the floor will greatly simplify standardized photography.

FRAMING

The images in this chart are marked with gridlines to assist in proper framing. These gridlines correspond to the descriptive text found under the "Framing" section for each photo series. The proper use of these guides will allow for consistent framing and magnification across patients of varying sizes.

Wherever a yellow line appears at one edge of an image, the photo should be framed by placing the appropriate anatomical landmark against that edge. Since magnification is kept constant for all patients, the landmarks found at the opposite edge of the frame may vary.

When an image is meant to be framed by positioning an anatomical landmark in the center of the frame (or one-quarter of the way from the edge), this is indicated by a dotted white line on the image.



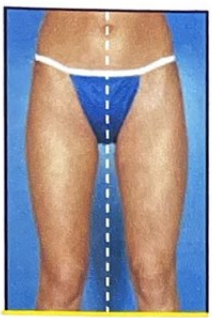
edge-oriented framing

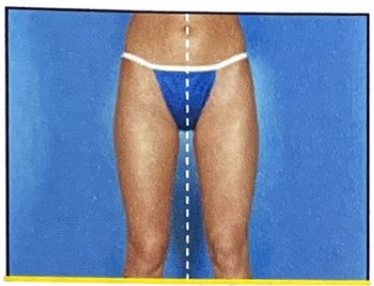
reference edge (yellow border) Align appropriate anatomical landmarks with this edge.

free edge (no yellow) Landmarks at this edge may vary from patient to patient.

center-oriented framing

Dotted white lines mark the vertical and/or horizontal center of the frame. This indicates that appropriate anatomical landmarks should be centered in the image. (In a full-face photo, for example, the ears are centered vertically and the whole head is centered horizontally.)





ASPECT RATIOS

The images in this photo guide all have an aspect ratio of 2-by-3 (i.e., they are two-thirds as wide as they are long). This is the aspect ratio of 35mm film and many digital cameras. In addition, each image is captured in either a vertical or a horizontal orientation in order to maximize the subject area relative to the background.

Depending on the specifics of the imaging system that is used, the aspect ratio may differ from that shown here. For example, video cameras and some digital cameras capture images in a 4-by-3 aspect ratio. Also, it is sometimes impractical and/or undesirable to capture images in both vertical and horizontal orientations.

For an aspect ratio other than 2-by-3, it is necessary to determine new target areas that capture the same 2-by-3 vertical 4-by-3 horizontal information. Once this is done, the framing notes and gridlines may be used in the normal manner. For example, the 2-by-3 target area for hips/thighs is 42cm x 63cm (vertical). For a video camera (4-by-3 horizontal aspect ratio), an appropriate target area would be 84cm x 63cm. This captures the same clinical information (63cm from the knees up) but extends the background on either side.

POSITIONING THE PATIENT AND CAMERA

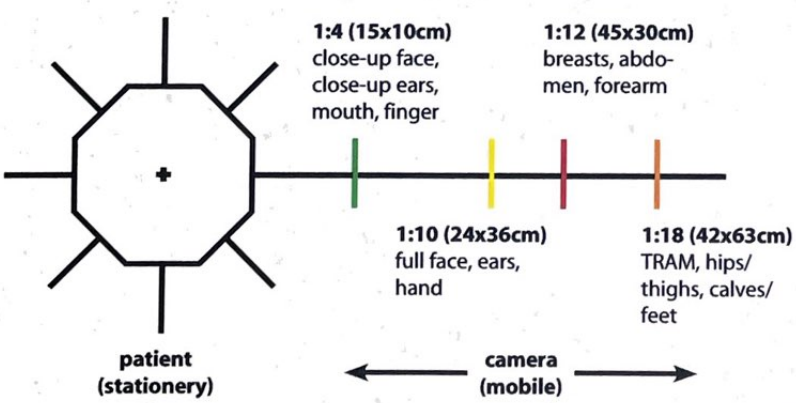
If clinical photos are to provide an accurate record of pre- and post-operative patient appearances, the relative positions of patient and camera must be kept constant. This is best accomplished through the use of strategically placed tape marks on the floor and walls of a photo studio or exam room.

The diagram below shows an overhead view of a suitable tape mark pattern. A 30cm octagon with radiating lines is used for positioning the patient. One line is extended out along the camera axis and marked at appropriate distances.

For body photographs, the patient stands with the outsides of the feet along opposite edges of the octagon. (The spacing of the feet helps create separation between the inner thighs.)

For facial photos, the patient sits on an adjustable height stool (with no back) placed over the center mark. With the stool adjusted to a comfortable height, the patient sits up straight with feet on either side of the appropriate radiating line. For a front view, the patient looks directly into the camera lens. For lateral or oblique views, the patient looks at a tape mark placed on the wall.

Holding the camera, the photographer sits, stands or kneels at one of the positions marked along the camera axis. For greater stability, the camera may be mounted to a tripod placed over the appropriate tape mark. Camera height is adjusted to match the height of the target area, with the lens barrel always parallel to the floor. It is important not to tilt the camera up or down when framing an image.



Camera stands are available that allow the camera to be moved up and down, forward and back, or left and right without tilting or swiveling. Such a stand greatly simplifies proper camera positioning.

QUICK TIPS FOR CLINICAL PHOTOGRAPHY

Taking a clinical photograph is not the same as taking a snapshot. A good clinical photograph should provide a maximum amount of pertinent medical information and a minimum of distraction.

To improve the quality of your patient photos, remember these simple rules:

• Photograph patients against a solid-colored background.
Use an appropriate backdrop. Light to medium blue is a good choice because it contrasts well with skin tones. Medium gray may also work well. Use a fabric drape or other non-reflective material.

• Remove distractions
Jewelry and clothing create an unnecessary distraction in patient photos. They should be removed from the area of interest prior to photography. For body photos, it is advisable to use special modesty garments (available from medical supply dealers) instead of the patient's underwear.

• Use controlled lighting
Available room lighting is not appropriate. Patients should be photographed using a flash system or studio strobes. Balanced cross-lighting (i.e., two strobes positioned symmetrically on either side of the camera) brings out surface texture without creating shadows that are overly harsh.

• Reduce cast shadows
The use of balanced lighting with diffusers can soften the shadows cast by the patient. To completely eliminate cast shadows, one or two additional lights may be aimed directly at the backdrop.

• Record settings
As much as possible, the same camera settings should be used for every patient. For settings that must be adjusted from patient to patient (such as exposure compensation), all values should be recorded, stored with the photos and referenced during post-op photography.

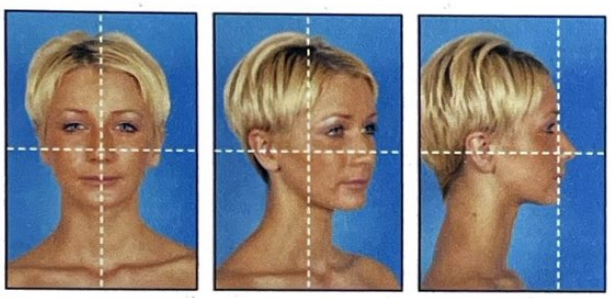
AMERICAN SOCIETY OF PLASTIC SURGEONS®

THE PLASTIC SURGERY FOUNDATION™

444 EAST ALGONQUIN ROAD
ARLINGTON HEIGHTS, IL 60005-4664
PLASTICSURGERY.ORG | THEPSF.ORG
847-228-9900

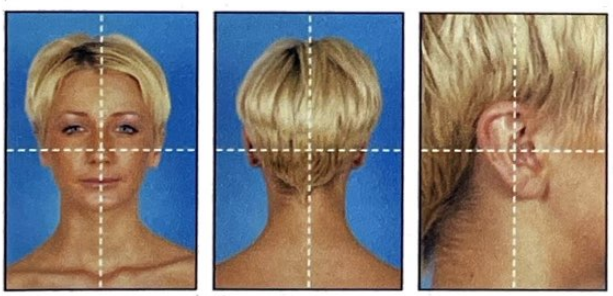
CLOSE-UP FACE

Target Area: 15x10cm (horizontal)
Reproduction Ratio: 1:4
Camera to Patient Distance:
Patient Preparation: Pull hair off face and behind ears (use black headband or small clips that hold hair without pulling), remove jewelry and eyeglasses, remove heavy makeup, cover shirt collar with black drape.
Patient Positioning: Seat patient on a stool adjusted to a comfortable height and placed at the center of a tape mark pattern. Patient should sit up straight with feet on either side of the appropriate tape mark. When turning for oblique and lateral views, patient should rotate entire body (shoulders and feet).
Framing: Place eyebrows (or proximal eyebrow) at top of frame. Center nose horizontally in all views.
Special Notes: For basal view, tip of nose should be aligned with upper eyelid crease.



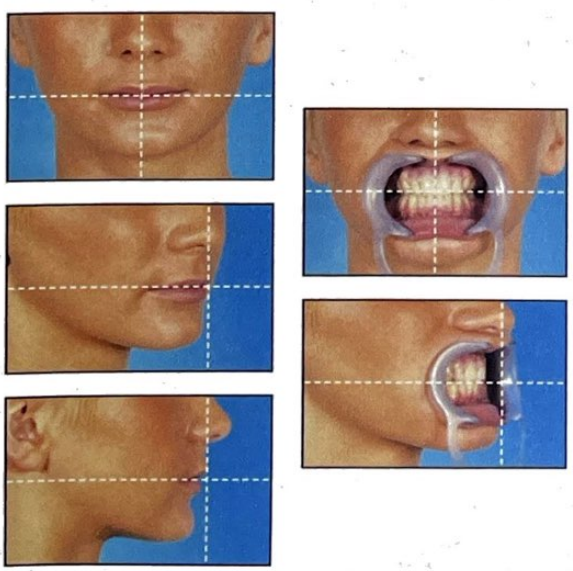
FULL FACE

Target Area: 24x36cm (vertical)
Reproduction Ratio: 1:10
Camera to Patient Distance:
Patient Preparation: Same as close-up face (see above)
Patient Positioning: Same as close-up face (see above)
Framing: Center ears vertically in all views. For frontal and oblique views, center entire head horizontally. For lateral views, place front of face 1/4 frame from edge.



EARS

Target Area: 24x36cm (vertical) / 10x15cm (vertical)
Reproduction Ratio: 1:10 / 1:4
Camera to Patient Distance:
Patient Preparation: Same as close-up face (see above)
Patient Positioning: Same as close-up face (see above)
Framing: Anterior and posterior views same as full face (see above). For close-up, center ear in frame.
Special Notes: Make sure hair is off of ears in all views.



MOUTH

Target Area: 15x10cm (horizontal)
Reproduction Ratio: 1:4
Camera to Patient Distance:
Patient Preparation: Pull hair off face and behind ears, remove lipstick and other makeup, remove any distracting jewelry, cover shirt collar with black drape.
Patient Positioning: Seat patient on a stool adjusted to a comfortable height and placed at the center of a tape mark pattern. Patient should sit up straight with feet on either side of the appropriate tape mark. When turning for oblique and lateral views, patient should rotate entire body (shoulders and feet).
Framing: Center mouth vertically in all views. In anterior views, center mouth horizontally. In oblique and lateral views, position lips 1/4 frame from edge.
Special Notes: For intraoral photographs, use flash heads positioned close to end of lens.

[redacted]

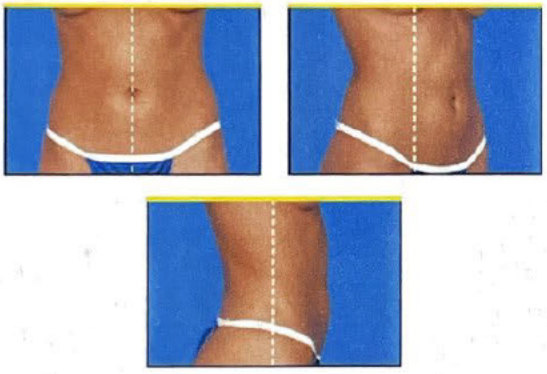
ABDOMINAL FLAP

Target Area: 42x63cm (vertical)
Reproduction Ratio: 1:18
Camera to Patient Distance:
Patient Preparation: Remove any visible jewelry. Remove gown completely. Patient should wear a photo garment.
Patient Positioning: Patient standing comfortably erect with arms at sides. Feet should be aligned with appropriate tape marks on floor. For oblique views, distal arm should be moved back slightly.
Framing: Position clavicles at top of frame. For frontal and oblique views, center torso horizontally. For lateral views, center mass of proximal breast horizontally.
Special Notes: Distal breast should not be visible in lateral views.

BREASTS

Target Area: 45x30cm (horizontal)
Reproduction Ratio: 1:12
Camera to Patient Distance:
Patient Preparation: Patient disrobed above the waist. Remove any visible jewelry.
Patient Positioning: Same as ABDOMINAL FLAP (see above).
Framing: Position clavicles at top of frame. For frontal and oblique views, center torso horizontally. For lateral views, center mass of proximal breast horizontally.
Special Notes: Distal breast should not be visible in lateral views.

[redacted]

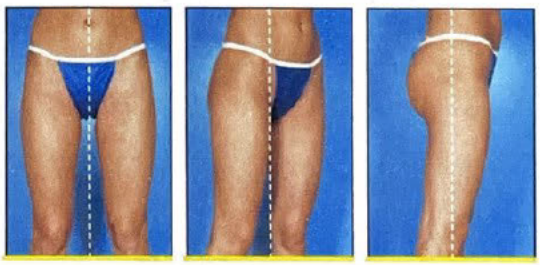


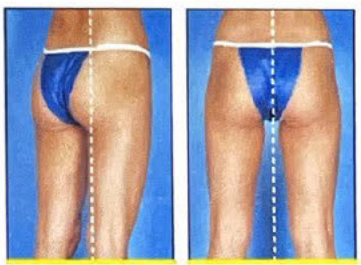
BODY CONTOURING

Target Area: 45x30cm (horizontal)
Reproduction Ratio: 1:12
Camera to Patient Distance:
Patient Preparation: Remove gown completely. Patient should wear a photo garment.
Patient Positioning: Patient standing comfortably erect with arms folded above breasts. Feet should be aligned with appropriate tape marks on floor.
Framing: Position inframammary fold at top of frame. Center torso horizontally.

HIPS/THIGHS

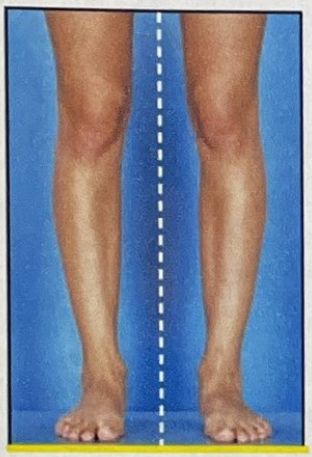
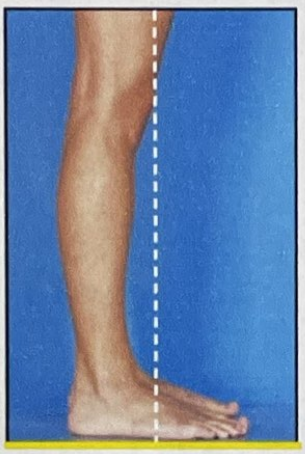
Target Area: 42x63cm (vertical)
Reproduction Ratio: 1:18
Camera to Patient Distance:
Patient Preparation: Remove gown completely. Patient should wear a photo garment.
Patient Positioning: Patient standing comfortably erect with arms folded above breasts. Feet should be at approximately shoulder width, aligned with appropriate tape marks on floor. (For larger patients, a wider stance may be required.)
Framing: Position knees at bottom of frame. Center hips horizontally.
Special Notes: Distal leg should not be visible in lateral views.





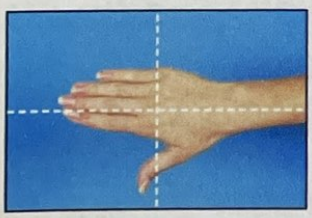
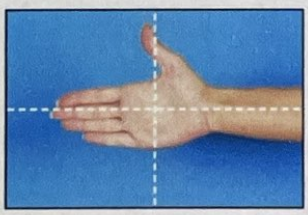
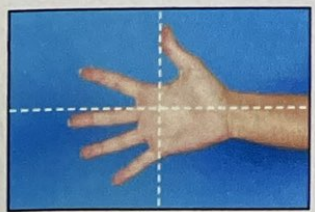
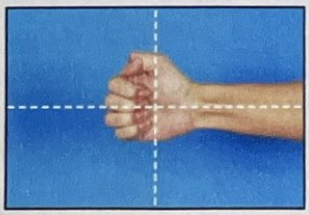
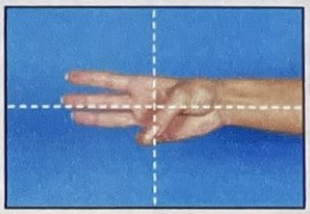
CALVES/FEET

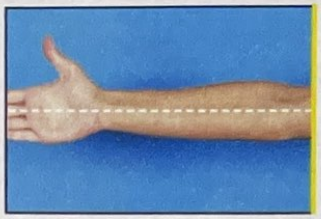
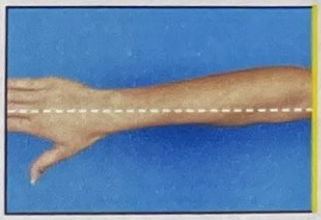
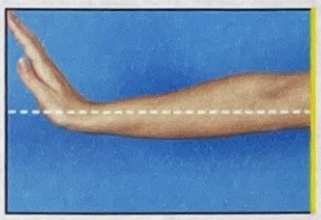
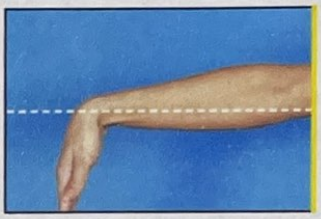
Target Area: 42x63cm (vertical)
Reproduction Ratio: 1:18
Camera to Patient Distance:
Patient Preparation: Patient disrobed below the waist. Remove any jewelry from ankles or toes. Remove nail polish, if needed.
Patient Positioning: Patient should stand on a step stage with feet at approximately shoulder width.
Framing: Position toes at bottom of frame. Center feet horizontally.
Special Notes: Distal leg should not be visible in lateral views.

HAND

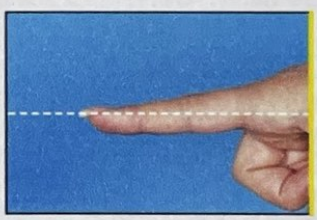
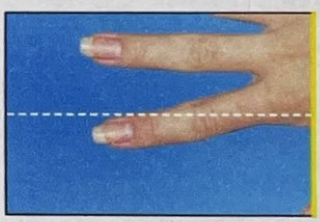
Target Area: 36x24cm (horizontal)
Reproduction Ratio: 1:10
Camera to Patient Distance:
Patient Preparation: Remove any jewelry from wrist or fingers.
Patient Positioning: Seat patient on a stool adjusted to a comfortable height and placed next to a tape mark pattern. Patient should extend hand horizontally above tape marks that are perpendicular to camera axis (i.e., tape marks for lateral views).
Framing: Center hand in frame.

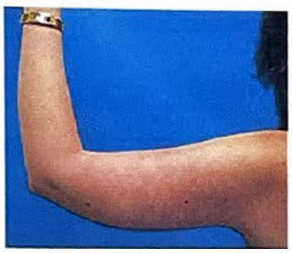
FOREARM

Target Area: 45x30cm (horizontal)
Reproduction Ratio: 1:12
Camera to Patient Distance:
Patient Preparation: Remove any jewelry from wrist or fingers. Remove nail polish.
Patient Positioning: Seat patient on a stool adjusted to a comfortable height and placed next to a tape mark pattern. Patient should extend hand horizontally above tape marks that are perpendicular to camera axis (i.e., tape marks for lateral views).
Framing: Place elbow at edge of frame and center forearm vertically.

FINGER

Target Area: 15x10cm (horizontal)
Reproduction Ratio: 1:4
Camera to Patient Distance:
Patient Preparation: Remove any jewelry from wrist or fingers. Remove nail polish, IF POSSIBLE.
Patient Positioning: Same as hand (see above).
Framing: Place metacarpophalangeal joint at edge of frame. Center finger vertically.



BRACHIOPLASTY/UPPER ARMS

Target area: 45x30cm (horizontal)
Reproduction ratio: 1:12
Camera-to-patient distance:
Patient preparation: Patient disrobed above the waist.
Patient positioning: Seat patient as in forearm. Extend arm in plane perpendicular to camera axis. Elbow flexed 90 degrees with palm facing the camera for anterior view and facing away for posterior view.
Framing: Center arm vertically in frame. Medial edge of frame extends to nipple and inferior edge of frame to inframammary fold.

VAGINOPLASTY

Target Area: 45x30cm (horizontal)
Reproduction Ratio: 1:12
Camera to Patient Distance:
Patient Preparation: Remove gown completely.
Patient Positioning: Supine; legs abducted with knees flexed; legs abducted, knees flexed, and labia majora retracted to demonstrate vestibulum and clitoris.
Framing: Place mons at top of frame and upper thighs at bottom of frame. Center genitalia horizontally.

[redacted]

[redacted]

PHALLOPLASTY

Target Area: 45x30cm (horizontal)
Reproduction Ratio: 1:12
Camera to Patient Distance:
Patient Preparation: Remove gown completely.
Patient Positioning: Supine; standing upright; standing upright with phallus retracted superiorly to demonstrate ventral phallus and scrotoplasty;
lateral view.
Framing: Place lower abdomen at top of frame and upper thighs at bottom of frame. Center genitalia horizontally.

METOIDIOPLASTY

Target Area: 45x30cm (horizontal)
Reproduction Ratio: 1:12
Camera to Patient Distance:
Patient Preparation: Remove gown completely.
Patient Positioning: Same as phalloplasty (see above).
Framing: Place lower abdomen at top of frame and upper thighs at bottom of frame. Center genitalia horizontally.

[redacted]